LN324-91

STUDY MANUAL

Manual 2 English
of 7 Manuals

COUNTER INTELLIGENCE

#849

Encl 2

PROLOGUE

The purpose of this booklet is to present basic information on the mission and activities of Counter Intelligence. But, with the understanding that the primary mission is to support the commanders of the armed forces. This booklet is dedicated to the concepts of Counter Intelligence in relation with its functional areas, the application of these functions, and a specific dedication and instructions on how to apply these functions. The terms "special agent of Counter Intelligence" (SA) refers to all those persons who conduct and contribute to the handling and gathering of information of the multi-disciplinary intelligence of the hostile services. This booklet is primarily oriented at those persons involved in the control and execution of the operations of CI. In like manner, this booklet has a very significant value for other members of the armed forces that function in the areas and services of security and other departments of intelligence.

COUNTER INTELLIGENCE
TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION TO COUNTER INTELLIGENCE

INTRODUCTION

Imagine a circle representing the effort of a total intelligence conducted by all the agencies of the Armed Forces. Inside this overall field, we find that counterintelligence is an integral part of the total intelligence effort.

DEVELOPMENT

DEFINITION OF COUNTERINTELLIGENCE:

Counterintelligence is defined as the activity or activities collectively organized by an intelligence service dedicated to obstruct the enemy's source of information by means of concealment, codes, crypto, censorship and other measures to deceive the enemy by using disinformation, trickery, etc.

The two measures used by Counterintelligence are DEFENSIVE or OFFENSIVE:

Defensive measures vary normally with the mission of the unit. An example of these measures are:

Counter-espionage

Counter-sabotage

Counter-subversion

Antiterrorism

Counter-terrorism

Intelligence consists of collection, transmission and dissemination of military data referring to possible or real enemy and/or to an area of operations. The military commander uses this intelligence in order to formulate his possible course of action and to select a course of action in particular in order to achieve the mission. Thus, the intelligence obtained is of vital importance to the commander and for the conduct of his mission.

Intelligence is also essential for the enemy as it is for us. The enemy also uses all sorts of measures at its disposal to become informed about our capabilities, vulnerabilities and probable cause of action, and also information about the meteorological conditions of the terrain.

Military Counter Intelligence is that part of Intelligence intended to deprive the enemy of this knowledge, and in this manner prevent the enemy activities of espionage, sabotage and subversion, as well as discover possible acts of an adverse nature, treason, or sedition among our own military forces.

Counter Intelligence is a significant aspect in both the strategic intelligence and combat, and is essential for the favorable application of two of the nine basic principles of war: security and surprise. The principles of war are:

Mass
Objective
Security
Surprise
Command
Offensive
Maneuver
Force economy
Simplicity.

Effective Counter Intelligence enhances the security and helps achieve surprise. Surprise depends not only on the intelligence obtained and the speed of movement, but also on the effective counter intelligence. Effort to prevent the enemy from obtaining data, reducing the risk that the command can suffer, provided it diminishes the enemy's capability of utilizing effectively its potential of combat against our Armed Forces. Thus, effective counter intelligence allows security of the unit.

DECEPTION:

Deception in combat is a military operation designed to conceal our dispositions, capabilities and intentions and deceive the enemy in such a way that it would be to his disadvantage and to our advantage.

Deception is designed to derail or deceive the enemy through manipulation, disinformation, or falsifying of evidence in order to induce a reaction in a way that is detrimental to his own interest.

In order for a deception operation to be successful, the enemy has to have the capability of collecting information that we would like him to get, so that we can react according to the information.

The enemy is given the opportunity to obtain information, and thus creating a deceptive picture. At the same time, counter intelligence goes into action in order to prevent the enemy from discovering the true purpose of the operation of deception and to avoid recognition of the true technical operation or the principle one, which is being supported by the deceptive operation mainly security.

QUESTION: Why can we consider a soldier as a counter intelligence agency?

ANSWER: An individual solder is an agent of the CI, since he can provide information on the activities of the intelligence of the enemy, including subversion. Much of the CI operations depends on the individual soldiers ability to adequately fulfill the security procedures, camouflage, observation and information system.

As a prisoner of war, the individual soldier is a soldier of operational information of the enemy. Therefore, the individual soldier receives training in the measures of escape and invasion, in case he is taken prisoner or that he finds himself behind enemy lines. Also he receives training to resist the interrogations of the enemy and adhere to his rights as a prisoner of war under the Geneva Convention.

All the units are agents of the CI and they too take measures of CI in order to deprive the enemy intelligence on our activities, operations and locations of this positions.

Every officer of the high command and every subordinate command in effect acts as a Counter Intelligence officer of the Joint High Command. For example, the transport officer aids the command with the Counter Intelligence aspects regarding the movement of transport; the health chief accesses the Counter Intelligence aspect regarding the location of the health installations.

Some units, such as the units of the censure, have special function of CI because of the nature of their assigned missions. The CI agent of the Army has the personal training as specialist in CI and is available for providing support in all the military operations.

Other government agencies, such as the agencies of intelligence of the Navy, the Air Force and the Defense Ministry, also use certain functions of CI that support the CI operations of the Army.

Keep in mind that kind of intelligence is necessary in both times of peace and war, since espionage, subversion and occasion sabotage are not only limited to conditions of time of war. All foreign countries, both enemy and friends, wish to obtain information regarding the Armed Forces, their assets, disposition, weapons, level of training and future plans for operations peace time as well as in time of war.

The range of the CI operation extends in proportion to the level of command.

At the division level the measure of CI generally have to do with military security.

CI operations at higher levels are similar to those of the inferior levels. Nevertheless, the operations have a broader range thanks to the greater number of units in the scope of their areas with a great volume of advance planning. The CI operations at superior levels include:

MILITARY SECURITY

SECURITY OF PORTS, BORDERS AND TRAVEL

CENSORSHIP

SPECIAL OPERATIONS

CIVILIAN SECURITY

Generally speaking, Counter Intelligence is a main part of the intelligence operation in the theater of operations.

Depriving the enemy of information regarding supplies, installations, nuclear weapon systems, means of transport, communications is vital in fulfillment of the mission in the zone of the theater of operations. The great territorial responsibility of this zone require extensive operation of the CI of all types.

COMMANDERS' RESPONSIBILITIES:

QUESTION: IN THE MILITARY UNIT, WHAT ARE THE THINGS THAT INTEREST THE ENEMY?

ANSWER: Military information.

Personnel.

Equipment and installations.

As in all aspects of the military unit, the commanders are responsible for the implementation and execution of all the measures of military Counter Intelligence to protect military information, personnel, material and installation within the unit.

The commander has his high command which can delegate the authority to carry out these functions; nevertheless, the responsibility rests with the commander.

The Counter Intelligence officer:

The auxiliary chief of the high command, C-2, is the officer of the high command responsible for the military information which also includes Counter Intelligence. This delegation of authority is given to the auxiliary chief of the high command, C-2, who has under his charge and responsibility of the high command regarding Central Intelligence and CI. The C-2 is responsible for the implementation and direction of all the measures of CI inside the command.

The planning of military Counter Intelligence is based on ability or capability of the enemy to obtain information regarding friendly activities. This planning includes adequate CI countermeasures to prevent the enemy from discovering the dispositions and activities that can reveal the intentions of the command or, if interrupted, could endanger the accomplishment of the mission.

According to the organization and the size of the command, there may be a CI official of the high command of the C-2. At the division or brigade level, the official of the CI normally is the chief of the section of security or the detachment of military intelligence that supports the division of the brigade. In other words, he wears two hats, as chief of the security section, and as the CI officer of the joint high command of the C-2.

CATEGORIES OF CI OPERATION

Generally, there are five categories of operations of CI conducted inside the theater of operation at which the C-2 is responsible or has direct interest. The categories are:

MILITARY SECURITY

CIVILIAN SECURITY

HARBOR, BORDER AND TRAVEL SECURITY

CENSORSHIP

SPECIAL OPERATION

MILITARY SECURITY

The military security encompasses measures taken by the command to protect itself from espionage, enemy civilians, supervision and sabotage and surprise. These include passive CI measures and active ones inside the Armed Forces and directly pertaining to the same and for specific military operations. Examples of military securities are:

SECRECY DISCIPLINE: This is the indoctrination/training on a continuous basis of all personnel against divulging of classified information that is not authorized or unclassified regarding military activities, and the use of patrol of security in areas frequented by military personnel.

SPECIAL PROTECTION OF CLASSIFIED MILITARY AND EQUIPMENT INFORMATION: This is the observation of the security measures, such as the security necessary inside the areas that contain information and classified equipment; introduction of a system of passes for entering critical areas; the conduct of studies in inspection of security to determine the strict observation of prescribed security measures.

SECURITY OF TROOP MOVEMENT: This keeps a certain connection with the secrecy discipline, preventing inappropriate comments by personnel in the unit given an order for movement; in returning mail dispatches of the unit in a certain period of time before the departure of the troops, and restricting all personnel in the area of the unit.

COUNTER SUBVERSION INSIDE THE ARMED FORCES: This is the overcoming of suppression of rumors and propaganda and the apprehension of subversive agents.

THE TECHNICAL MEASURES AS REQUIRED IN THE COMBAT ZONES: This is the use of the technical troops for the apprehension of the resistance groups, to help reduce the intelligence subjective and the mop up operations of the guerilla units.

TRANSMISSION SECURITY: Listening to the administration communication networks, command operation of intelligence.

SPECIAL HANDLING OF ESCAPEES AND EVADERS: This type of person needs to be debriefed to obtain the immediate intelligence information. It is of great importance to make sure that the escapee or evader is not an enemy agent.

CIVILIAN SECURITY: In all cases the mission of the military forces has priority over the well being of the civilians in the area. Examples of the civilian security measures are:

Systematic registering of the civilian personnel, including the neutral foreigners and enemies: This is done by the civilian affairs agency and includes the distribution of rationing cards, work permits, travel permits and permits for crossing borders.

Control of the circulation of the civilian personnel and refugees: This is a very important matter: All civilian personnel must be kept away from the advance combat zones, which will help prevent their easily finding out about our forces and inform enemy agents of espionage or sabotage. Also, all civilian personnel is to be kept at a distance from the major route of supply to make it easier for the military transport and prevent enemy agents from infiltrating the military zone.

Curfew: Keeping the public away from the streets and routes after certain hours, thus restricting the movements of enemy agents.

Surveillance of suspect political groups: One should find out whether other groups are sympathetic to enemy cause. Such groups must always be considered potential agents.

Investigation of workers security: Local workers employed by the Armed Forces should be investigated to avoid infiltration of enemy agents in areas and military units. This include the service personnel of the countryside, truck drivers and current workers, and interpreters, translators, etc.

Distribution of passes and permits. Passes and permits should be strictly controlled and reviewed frequently to avoid forgery. Passes and permits for travel are normally distributed to government functionaries, political agencies, doctors and workers of public services.

Control of international commerce: Control of commerce in neutral states. Experience has proven that many commercial companies are in effect spy agencies that use the company as a cover or front of their operation. The profits from the trade of these companies can be and is used to pay for the expenses of espionage operations.

Surveillance of consuls and neutral/high command diplomats: It is possible that people of this category are using their diplomatic immunity to act as couriers for an enemy country.

SECURITY OF HARBORS, BORDERS AND TRAVEL: Consists of special applications of both the neutral security measures as well as civilians for the control of Counter Intelligence in entry ports and ports of departure for borders and international lines; all movements of a non-military character, of entry and departure in the theater of operations.

SECURITY CONTROL OF MARITIME HARBORS: This is the responsibility of the Navy and control should be coordinated with the Navy.

SECURITY CONTROL OF AIRPORTS: This is the responsibility of the Air Force and control should be coordinated with the Air Force.

ESTABLISHMENT OF CROSSING POINTS ON THE BORDER: Normal routes of movement should be directed to points of crossing located strategically. These points of crossing should be controlled by military personnel with the help of local and national agencies as necessary.

SECURITY CONTROL OF THE MERCHANT MARINE AND THE CREWS OF COMMERCIAL AIRCRAFT: This is important due to such individuals who by virtue of their occupation can enter and depart legally and frequently from the country and such individuals can be used as pretext for carrying out fraud operations (diplomatic pouch).

INVESTIGATION OF SECURITY AND CONTROL OF PERSONS WHO LIVE AT THE BORDERS: Personnel in this category, for example, the farmers who live at the border and the entire front can be on the border, personnel living on one side of the border and working on the other side.

CONTROL OF DISEMBARKATION PASSES AND PASSES FOR LANDING, AND FISHING PERMITS: The fishing boats and small craft of a similar nature that operate in very shallow water and thus have the capability of landing enemy agents at any point on the coast of the country where the military operations take place.

CENSORSHIP: Censorship is the control and elimination of communication with a double purposes: First, to avoid the transmission of information that can be of interest in helping the enemy; and secondly, to collect and propagate valuable information in the service of intelligence that helps the war effort. The term communication includes all types of postal material, regardless of class; means of electrical communication and any other tangible form of communication that can be carried by a person, carried in luggage, or among personal effects or in any other way can be transmitted from the area where the censorship is taking place.

THERE ARE FOUR TYPES OF CENSORSHIP IMPLEMENTED DURING WAR CONDITIONS WHICH ARE:

Censorship of the Armed Forces: This censorship is the control and examination of all communications sent and received by personnel under the jurisdiction of the Armed Forces, which include assigned military personnel, the civilians that can be employed and added to the same. This includes all war correspondents, representatives of the Red Cross and technical representatives of the factories.

Civilian Censorship: The civilian censorship is the control and examination of all communication of the national and civilian population of the common goal and transit or circulate in a territory which cannot be liberated, occupied or controlled by the Armed Forces.

Press Censorship: Press censorship is a division of the security of the news material and other media that are used, including maintenance of security. This applies primarily to the work that is done by the war correspondents, radio commentators and press photographers, and also includes any material prepared on a possible location by the personnel under the jurisdiction of the Armed Forces.

Censorship of Prisoners or War: Censorship of prisoners of war is control and examination of the political communication of the prisoners of war and the civilian detainees under the jurisdiction of the Armed Forces.

SPECIAL OPERATIONS: The final category is the special operations. Operations that come under this category will be discussed and planned according to the specifications of the commander in keeping with the planning within the SOP of CI.

CHAPTER 2

OPERATIONS SECURITY [OPSEC]

INTRODUCTION

Operations security is one of the keys for achieving the two war principles: surprise and security. A military force has the advantage when he can surprise the enemy. In order to achieve this goal, those military forces must protect their operations and activities with a continuous implementation of a security plan that is healthy and effective. The purpose of OPSEC is to protect the military operations and their activities by negating the indicators military forces plans and their intentions vis-a-vis the enemy forces. In other words, the enemy commander should not know or recognize how, when, where, why and what operations our forces are about to undertake, until it is too late for the enemy to react effectively against our operations.

OPSEC is the duty of the commander, together with each individual at all levels of command. The commander determines which are the measures of OPSEC which should be implemented and the duration of each event. Equally, they should determine the level of risk that they should be willing to accept. The elements of intelligence (SD) provide information about enemy threat. The operation elements (S3) direct the program of OPSEC and recommend measures for OPSEC. The units of each individual implement those OPSEC procedures. In order to attain a good OPSEC program, commanders and the members of the joint command, and each individual should be trained in the proper use of the procedures and techniques of OPSEC.

This teaching plan provides a guide for the procedures to be used by the technical units in the OPSEC program. Described OPSEC and provides doctrinaire direction for the future instructors and trainers.

What is OPSEC?

GENERAL

In order for our military forces to be successful against enemy forces, information about the activities of our units or plans and operations should be denied to the enemy until it is too late for him to react effectively.

OPSEC does not occur by itself. Our military forces have to create the right condition for a good OPSEC program since OPSEC is an integral part of all the operations and activities. The OPSEC program can be good because it was implemented effectively in each unit; or it can be a program without effectiveness because the members of the unit did not know the importance of the program and does not know what it requires.

OPSEC IS ALL ACTION TAKEN BY THE COMMAND TO DENY INFORMATION TO THE ENEMY ON OUR ACTIVITIES OR MILITARY OPERATIONS

Generally, OPSEC includes coordination of various techniques and procedures that deny information to the enemy. It is the common sense applied systematically to the situation of a unit or a mission. The result is the security of the military forces. This requires a total effort of integration by all commanders, and the members of the team, and the units and each individual. Under the umbrella of OPSEC, there exist basically three types of action.

COUNTER SURVEILLANCE - These activities are taken to protect the true purpose of our operations and activities.

COUNTER MEASURES - Those actions taken to eliminate and reduce the enemy threat and its capability of intelligence and electronic warfare against our military forces.

DECEPTION - Those actions taken to create the false image of our activities and operations.

COUNTERSURVEILLANCE

SIGNAL SECURITY (SIGSEC)

The signal security includes communication security (COMSEC) and electronic security (ELESEC).

COMSEC includes those measures taken to deny the enemy information on our telecommunications. This includes the cryptographic security, transmissions security, physical security of COMSEC information, and measures to assure the authenticity of the communications.

ELESEC is the protection of the electromagnetic transmission, which includes the communication apparatus. This includes such measures as standard operations procedures which have been approved, appropriate search, maintenance procedures, and training programs.

ELECTRONIC COUNTER COUNTERMEASURES

Electronic counter countermeasures (ECCM) are various measures taken to protect the electronic transmissions of our military forces and the detection capacity, recognizing and identifying the enemy. This includes the proper use of the command post of the motor, situating the antennas, concealing and distancing the antennas, a check of the equipment to secure and make sure that there is no radioactive radiation, and training.

A good electronic counter countermeasure program must ensure the effective use of the electromagnetic systems of our military forces.

INFORMATION SECURITY (DOCUMENTS)

Information security INFSEC is the protection of information of value for the enemy forces. This includes two types of information, classified and unclassified. Some examples are the dispatch documents, requisitions (orders), plans, orders (directives), reports, charts (maps), map covering material, and dissemination of verbal information, and the press that may have an adverse effect on national security and the operation of friendly military forces.

PHYSICAL SECURITY

Physical security (PHYSEC) is the protection of the installations, command post and their activities, etc., by the members of the Armed Forces, dogs, and other necessary measures for the restriction and protection of the area. Some measures include barriers of the perimeters, detective lights, marked copies of the keys or combinations, bolting mechanism, alarm systems for the control of intrusion, personal identification, controlled access, and controlled movement. The PHYSEC also allows the protection against espionage, sabotage and robbery.

STANDARD OPERATION PROCEDURES (SOP)

As a general rule, the countersurveillance procedures such as camouflage, concealing and the use of color, light and noise, are concealment measures discussed in the SOP. The SOP also covers the manner in which the unit utilizes buildings, roofs, highways and its equipment.

COUNTER MEASURES

Counter measures are selected, recommended and planned in order to overcome the specific aspects for the operation of intelligence of the enemy. Once a vulnerability has been identified and the risk is determined to exist, a counter measure is designed specifically for this threat in order to avoid exploitation of said vulnerability by the enemy. The counter measures can be anything from deception to the destruction of the capability of the enemy's means. The counter measures also include appropriate measures to discover the vulnerability of the friendly force. For example, the use of smoke, or the use of flak in critical moments. The deception operation also can be planned.

DECEPTION OPERATIONS

Deception operations (DECOP) are carried out in order to deceive the enemy. These operations include:

Handling of Electronic signatures

Distortion of the friendly activities in order not to make the real objective known.

Falsifying material, and placed wherever it can be captured or photographed by the enemy.

Simulated maneuvers

Demonstrations

Simulated equipment

Deception operations can be conducted when the commander sees an opportunity to deceive the enemy.

Also, deception can be required when the countersurveillance ??? operations are not sufficient to disorient the enemy so that the operation may be successful. In any case, knowledge of the friendly military forces provided by security analysis is necessary in order to create a credible deception plan.

SECURITY ANALYSIS

Security analysis is done in order to support the countersurveillance and counter measures. OPSEC depends on the commander and his personnel being informed of a threat that they will confront, in the patterns, weaknesses and profiles of the friendly force. Intelligence analysts provides information on the enemy; the analyst assigned to OPSEC section determine which unit or activity of the friendly forces are vulnerable, and why. The OPSEC analyst provides the commander and the operators with a risk estimate; this is based on the efforts of the aggregate of intelligence of the enemy and the activities of the friendly forces that are known. They can recommend procedures or procedures of countersurveillance and counter measures.

OPSEC is a condition.

Generally, OPSEC is a condition that seeks to attain security or safety of the friendly forces. It involves a variety of activities for concealing the friendly units, or to deceive the capabilities of the enemy analyst and commander in regard to intelligence gathering. These activities (under the category of countersurveillance, counter measures and deception) can be accomplished independently by members of each unit. But it is the integration of these activities by the commanders and the operation officer, which transforms the OPSEC program for a unit and provides security for the operations. The elements of security such as SIGSEC, counter intelligence, military police, and the personnel of each unit, provide the necessary support to create good conditions for OPSEC in the installations.

THE THREAT

COLLECTIVE CAPABILITIES OF THE ENEMY

HUMAN RESOURCES	ELECTRONIC RESOURCES	IMAGE RESOURCES
Agents	INTELSEN/GE	Photography
Infiltrators	-- Radio interception	Infrared (close and distant)
Reconnaissance Unit	--Radar interception	Night vision equipment
Combat Unit	--Interference equipment	Image amplifiers
Patrol	--Radar surveillance	Visual
Prisoners of war	--Telesensors	SLAR
Refugees	--Acoustics	

Figure 1

The intelligence threat against our Armed Forces vary from place to place, according to operations, missions, contingency plan and the level of sophistication of the enemy. Therefore, the units to receive information about the threat in specific situations in the local sections of intelligence. It is expected that the enemy units will utilize all of their capabilities of collecting information, as is shown in Figure 1, when they confront our forces.

The enemy is particularly interested in the different echelons of our military forces: which are the capabilities of the unit; such as, their fire power, communications, detection capabilities, logistic support, but in the same way are interested in the location, movements, and intentions of our military forces. The capability of the threat that is discussed in the classrooms and the practical exercises of the units should be based on the capabilities of the enemy and the ones that can have be a fundamental threat in the operation activities of the unit involved. In other words, the OPSEC program was developed in order to counteract the specific threats against the military unit involved.

OPERATIONAL GUIDE

GENERAL

The OPSEC program is conducted by the commander and led by the operations officer as part of the operations of each unit. Each unit can have an effective OPSEC program with only the coordinated forces of the commander, members of the task force and the troops, and the use of various activities of security and intelligence.

NUCLEUS OF THE OPSEC OPERATIONS

Operations Officer

G1/S1

G3/S3

SIGSEC

Commander

Troops

Counter espionage

G3/S3

MILITARY INTELLIGENCE

The OPSEC program is designed to function with the characteristics of the technical operations, and the requirements of each organization. Each unit takes the necessary steps to provide the security and maintain the surprise - keep the enemy without knowledge of what our military forces are doing. For this reason, OPSEC should be taught in all the military schools at all levels, and established in the doctrinaire literature of each organization and its operations. Each manual should describe how military forces can improve the security of their operations.

In order for the OPSEC program to be effective, the tactical units should:

Be established by the commander, and led by the operations officer of the support of the local intelligence officer.

Be based on the operational requirements of the unit.

Be imaginative and adaptable for certain changes.

Be designed to deny valuable information to the enemy regarding activities and operation.

Be compelled at all levels by the commander in the plans and training, so that the program can function in operations situations.

OPSEC SUPPORT

The OPSEC support is provided by the unit or sections of the OPSEC which are found in the organizations of military intelligence. The OPSEC teams are specialists in security signals in the counter intelligence and should be put in direct support of the combat brigade, support division commands and the artillery units. These teams support the unit determining the vulnerability of each unit, to assist the subordinate units and maintaining the most current data regarding enemy threats and evaluation of vulnerabilities of such threats. The support units of OPSEC participate in the conduct of evaluation of OPSEC. They also recommend certain ways of protecting the procedures which could provide indicators to the enemy.

The security specialists help in the development of the plans and procedures of OPSEC, maintaining the archives of OPSEC, and recommending the deception measures. Commanders can also obtain the support of the units of OPSEC at the highest echelons of the high command of the Armed Forces. This support includes services such as the signal security, computerization security, counter measures of technical surveillance, counter intelligence investigations and inspection of cryptographic installations.

THE OPSEC PROCESS

OPSEC is a continuous process of planning, collecting information, analyzing and forming, changing data base, issuing orders and instructions and execution.

OPSEC PROCESS

Planning the gathering --->Information gathering--->Analyzing

Report on results

Report

Executing orders <---Issuing orders and instructions <------Revising the data Base

NOTE: Once started, the OPSEC process is continuous and more than one section can do it at any moment.

The OPSEC process is done in a sequence of planning, execution and reporting the results. The process begins with information already known of the data base and continues in a logical way resulting from the assessment, recommendation and operation plan. The plan is carried out by the units. The OPSEC measures are monitored by members of the different unit and by elements of the CI to verify the effectiveness of the OPSEC measures. The commander and the operations officer take action to correct the vulnerabilities based on the different reports. The process can be illustrated as follows:

THE OPSEC PROCESS

	S3/D3	S2/D2
Based on Data base	OPSEC profile or Condition of our forces	Estimate of the enemy intelligence threat
and Commander guideline	countersurveillance in effect	

The Concept of the Commander of the mission or operation

PLANNING	--Determine the sensitive aspects of the operation --Develop the essential elements of friendly information (EEFI) --Advise on our vulnerabilities --Analyze the risk --Determine countermeasures and requirements of deception --Estimate of OPSEC (written or orally) --OPSEC plan (written or orally) --Deception plan (written or orally)
IMPLEMENTATION	--Units implement Operational Plan (With the OPSEC plan as an Annex) --Counterintelligence elements supervise the OPSEC plan --Inform on indicators that can influence the operations --Effectiveness of OPSEC program is evaluated
RESULTS	--Counterintelligence elements inform the commander and the operations officer orally or in a written report.

Figure 1

THE DATA BASE

Data base for the planning of OPSEC is maintained by the CI section. This information on our units and enemy capability for gathering information is always in the process of evaluation and change.

The intelligence section informs the CI element regarding the capability of the element to collect information. This information about the enemy is important because:

Time is not wasted advising an erroneous threat.

Counter measures are not assigned to indicators which the enemy does not have the capability to collect.

Counter measures are assigned to counteract the capabilities of the enemy to collect information on our activities.

The CI section establishes the data base to develop the indicators, the signatures, the patterns and the profile of our forces. This information indicates how our units appear in the battlefield -- the way they operate, how they communicate, how they are supplied, etc. The information about our own unit is important for the planning of our operations because:

It determines the essential elements of information on our forces and our vulnerabilities.

Counter measures are applicable to the units which need them.

In carrying out and providing advice for OPSEC measures.

Deception can be done effectively. The use of deception depends on common sense, precise information about enemy intelligence and our involved units. For example, the units which use deception have to demonstrate indicators, signatures, patterns and profiles showing the same characteristics as the type of unit they are trying to imitate.

COMMANDER GUIDE

The concept of the operation and the mission of the commander provides the direction and guideline for the OPSEC plan. The commander can order certain general measures of OPSEC or perceive specific procedures of security during operation. For example, it can establish measures for protecting the revealing of unit movement, supplies and use of radio. The commander should announce which part of the operation should be protected for the operation to succeed.

PLANNING

The C3/S3 is assisted by the CI section and other high staff and general staff officers, realizing the plan described in Figure 1. Although the different aspects of the planning might not be completed in detail, each one should be completed as much as possible in a given time.

Determine the Sensitive Aspects of the Operation

Take note of the information which if known by the enemy provides indicators that reveal our operation. Operational indicators and physical characteristics are compared constantly with the operation. Once this is done the planners can --

Determine the Essential Elements of the Elements of Friendly Information (EEFI)

The essential element of friendly information is information that if it falls in the hands of the enemy, our operations will fail. The EEFI reflect the concern of the commander regarding areas that need security. The CI agents use the EEFI to identify and inform regarding vulnerabilities. The unit uses the EEFI to plan operations of countersurveillance.

Advice on Our Vulnerabilities

Noting the EEFIs, the CI sections begin to advise on our vulnerabilities. The CI agents identify the units and activities that are most vulnerable and detectable by enemy intelligence. This step is necessary for --

Risk Analysis

Risk analysis is a process that compares our vulnerabilities with the enemy capabilities for gathering of collect.

The CI agent identifies indicators that if detected would result in the divulging of important combat intelligence regarding our operations. The purpose is to identify the risk and determine what can be done to reduce them. This includes an evaluation of the operation of countersurveillance and counter measures actually in effect for determining what more needs to be done. The units always employ procedures of counter surveillance. The units separate and evaluate the effectiveness of countersurveillance as they receive new information. Based on the new information, they can decide and adjust the measures for countersurveillance in order to focus on certain techniques and procedures. This process continues throughout the CI agents structure.

Determine the Counter Measures

Counter measures are used to protecting these indicators and EEFI which are most vulnerable for enemy detection, as a result the counter surveillance measures which are not adequate. Generally there are five options:

Counter measures are not necessary

Applying a counter measure

Stop the activity

Employ deception operations

Change the operation

Counter measures are not necessary under the following conditions:

A indicator cannot be detected by the enemy

If it is detected, the indicator supports the deception plan.

The commander decides to accept the risk.

The use of counter measures in deception requires common sense, information over our units and knowledge of the capabilities of the enemy to gather intelligence. The specific counter measures are directed towards the capabilities of the enemy in order to collect information.

Counter measures may include the physical destruction of the enemy's collection measures. If this is the case, the S3, in accordance with the commander, has to react quickly in order to counteract the enemy's gathering capability. For example, it is known that an enemy reconnaissance patrol is collecting enough information regarding our operation, the S3 can recommend the increase of combat patrols to destroy the reconnaissance element.

Deception

The planning of deception is integral in the planning operations. A deception plan can be done because it is a good idea for a specific operation; because it is a requirement to support a plan of deception at a higher level as part of the measure against the enemy intelligence threat. In any case, deception and the OPSEC are inseparable. In order to use deception successfully, a unit has to have a good knowledge of all of the aspects of OPSEC.

Deception is designed to deceive the enemy by means of manipulation, distortion, making him react in a way that is detrimental to his interest. In order for a plan of deception to function, certain conditions have to exist:

-- The plan of deception should be credible. The concept of deception should be carried out in conjunction with the concepts of operation. Whenever possible, the operation activities should support the plan of deception.

-- The deception should be part of the technical situation.

-- The enemy should be given the opportunity to react to deception.

-- One should consider all the information gathering capabilities of the enemy. There is no point in deceiving an enemy resource if it is detected by another resource. The success depends on the good knowledge of the characteristics, capabilities and the use of intelligence systems of the enemy.

-- The units involved in the deception have to accomplish their different missions. This may not require anything special if the unit is doing its normal mission. It is possible that it may have enough information and equipment to project a false image. The subordinate units have to support the plan of deception of the superior units.

Deception requires good intelligence, OPSEC and an operational implementation in order for it to be successful. Intelligence units inform regarding information gathering capabilities of the enemy and possible reactions. The CI section informs regarding indicators, signatures, patterns and profiles of the units involving deception; and the operations sections applies the deception plan of the combat operations. A satisfactory OPSEC program needs to be established in order for the deception to be successful.

INDICATORS, SIGNATURES, PATTERNS AND PROFILES

General

All the armies have their ways of operating. The normal operating procedures, the field manuals, the training instructions, and other local instructions result in similar units functioning in a similar way. The effort of maintaining the similarities and functioning adds to the effectiveness and efficiencies of the units. Its weakness is that the units become stereotypical units, and consequently more predictable. This causes that the analyst of any intelligence can interpret more easily the indicators, signatures, patterns and profiles of our military forces.

The commanders and the operation officers should examine and study carefully how to conduct their military operations. They need to know if they are conducting operations in the same way each time there is an operation, and advise on the manner the operation should be conducted. This means that they should revise the actions that occur during the planning phase, execution and the debriefing after the combat drills. It could be that a comparison of the activities of various combat drills is necessary.

INDICATORS

Indicators are activities that may contribute to determine a course of action of our military forces. When preparing combat operations, it is virtually impossible for a military unit to hide or avoid giving out indicators. Certain activities must be conducted. Some of these activities are essential for the operations -- others can be directed by the commander or by standard operational procedures of the operations. In many cases, these activities might be detected by the enemy and used to predict possible courses of action.

Identifying and interpreting specific indicators is a critical task for the intelligence operations, either for the enemy of for our own armed forces. The intelligence personnel looks for indicators, analyze the, and make an estimate of the capabilities, vulnerabilities and intentions. These analyses have become a requirement for information, plans, and eventually provide the basis for directives and orders.

Identifying the critical activities of the military forces could indicate the existence of specific capabilities or vulnerabilities, or the adjustment of a particular course of action. Determining which indicator is important, could be the result of previous action analysis. The lack of action is as important, in certain cases, as actions already taken. For example, if a unit does nor normally deploy its attack artillery equipment, this information is important for the analysts to include it in their estimate. In any case, the indicators that arise requires a concrete knowledge of the organization, equipment, doctrine of the tactics, the command personalities, and the logistic methods, as well as the characteristics of the operations. Indicators are not abstract events. The indicators are activities that result from the military operations.

Indicators are potential tools for each commander. The indicators are probabilities in nature, which represent activities that might occur in the military operations. The interpretations of the indicators require knowledge of the enemy and the current situation. Some indicators are mentioned below. It is not intended to be a complete list, or applicable to all situations.

Possible Attack Indicators

-- Concentration of mechanized elements, tanks, artillery, and logistic support.

-- Delivery of combat elements (mechanized, tanks, anti-tank) in echelons.

-- Deployment of tanks, guns, cars to the front units.

-- Extensive preparation of artillery.

-- Artillery positions very much to the front and in concentration.

-- Extensive patrol activity.

-- Change in the level of communications, crypto, codes and frequency.

-- Placement of the air defense forces beyond the normal front.

-- Logistics activities, reinforcement and extensive replacement.

-- Relocation of support unit at the front.

Possible Defense Indicators

-- Withdrawal of defense positions before onset of battle.

-- Successive local counterattacks with limited objective.

-- Counterattack is suppressed before regaining positions.

-- Extensive preparation of field fortifications and mined fields.

-- Firing positions in the front are used; the long-range firing is started.

-- Movement to the rear of long-range artillery equipment and logistics echelons.

-- Destruction of bridges, communication facilities and other military equipment.

SIGNATURES

The signatures are a result of the presence of a unit or activity in the battlefield. The signatures are detected because several units have different equipment, vary in size, emit different electronic signals, and have different noises and heat sources. The detection of the individual signatures could be grouped by analysts to point out the installations, units, or activities.

In general, these are the categories applied to the units: visual, acoustic, infrared, and electromagnetic. Each one of these areas are discussed individually. Have in mind, however, that the enemy will try to exploit several individual signatures grouping them in order to determine a signature for the unit. Usually, action is not undertaken as a result of the detecting only one signature. With exception of the detection of critical areas, which can result of the detection, identification and location of a signature. The critical areas are key activities such as command posts, communications facilities and systems, some equipment and its surveillance systems. The detection of these areas reduces the ability of a military force to conduct military operations. However, the longer the critical areas are exposed, the easier would be for the enemy to detect, identify, locate, attack and destroy these critical areas.

VISUAL

Visual signatures are detected through light photography and by human eyesight, assisted or unassisted. Visual signatures are equipment, location of personnel, activity patters, and the frequency of these activities. Also, some of these visual signatures include vehicle movement, tanks, vehicle marking, uniform markings, etc. Theoretically, a target is detected when it is seen by a human eye. The targets might be detected and identified by using photography by --

-- Its distinct form, or recognizable patters, form, style, size, design, shadow, and its dimensions of height and depth.

-- A distinct deployment system, possibly involving other targets.

-- The color, hue, shine, tone and texture of the target.

It is possible to detect a target without having to identify it. Detection is the discovery of a target or activity, while identification requires an additional step -- to establish what the target is, what it does, or the capabilities of such target. The violence, confusion, and the darkness in the battlefield introduces variables that might prevent identification or detection of military targets.

Some studies point out that the visual detection is affected by the following:

-- The size of the target and the time it has been exposed to sight.

-- The degree to which the target has been camouflaged or covered.

-- Light variation, visibility and weather.

-- Number of targets -- the more targets there are, it is more difficult to identify them correctly.

-- Target distance - the longer the distance the more difficult to identify the target correctly.

-- The contrast of the target against the background -- the less contrast there is, the more difficult it is to identify the target.

Some factors help the probability of visual detection. For example, the probability of detection is increased by knowing previously that a target is in a particular area. The probability of detection and identification is also augmented if the target detected in a particular area is associated with other targets in the vicinity, in other words, find a known target and search for similar ones in the area. For example, if a tank repair vehicle is detected in an area, look for tank units or mechanized units in the vicinity.

The identification and visual detection can be enhanced with the use of photography. Visual location of ground and air observers, of which there is no specific identification, can be used to lead photographic reconnaissance missions. Unlike the location in one site only, or having a short view of the target, photographs provide the opportunity to enlarge and study specific areas and equipment. Photography is limited mainly because it provides the record of an area as it was at the moment the photograph was taken.

ACOUSTIC (SOUND)

The acoustic signatures come in two types: The first are noises produced during battle by explosives and rifle firing. The second sound is associated with the noise of certain military functions - such as vehicles, equipment and the activities of the installation. The acoustic signatures are detected by human hearing, sound detection equipment, or special devices that magnify the sound.

Acoustic sounds could be very significant because different equipment and guns have a unique sound. These signatures have considerable importance for planning countersurveillance, countermeasures and deception. The forces try to prevent escape of signatures in order to reinforce security; a deception plan must sound as if it were an actual unit.

The noises produced by operations are affected by the weather conditions, terrain, atmospheric conditions, and the propagation of sound. The relative direction of wind, the amount of wind, the temperature and humidity influence the quality of sound. In general, the sound travels better when projected by the wind, when humidity is relatively high, and during nighttime.

The enemy is not expected to react only to what he hears. The sound only serves to alert us on what is happening. The acoustic signature, unlike the visual signature that can stand by itself, normally is used to support other sensors.

The acoustic sounds are integrated with other information to enhance intelligence. But have in mind that under certain circumstances, the sound can travel long distances. While the enemy cannot distinguish between an M-60 tank and an APC, the sound can alert him that there is movement in the vicinity.

INFRARED (IR)

The infrared signatures are those not visible by the eye. It is the heat, or light, produced by equipment, person, unit or activity. The infrared signatures can be detected with the use of several specialized equipment.

The infrared surveillance equipment vary from the individual optical device to sophisticated aerial systems. Under favorable conditions, the systems that have been improved will be able to produce images that distinguish between the equipment of the same quality and type.

The tactical infrared equipment come in two categories -- active and passive. The active equipment require that the potential target be illuminated by infrared sources -- light sent in infrared frequencies. These devices are susceptible of being detected because they emit a distinct and identifiable signature. The enemy sensors can locate the active sources. The passive devices detect the infrared radiation of any of these two sources: emissions created by the target or solar energy reflected by the target. These devices are more applicable to play the role of surveillance because the equipment does not produce an identifiable signature. The passive devices are vulnerable to detection at the level at which their power sources are detectable.

The majority of the military equipment emit an infrared signature of some type. The equipment more vulnerable to infrared detection are those that produce a high degree of heat, such as, tanks, trucks, long guns, generators, air conditioners, furnaces, aircraft, maintenance facilities, artillery fire, kitchen areas, landing areas and assembly points.

Infrared surveillance has limitations. Humidity, fog, and clouds can cause serious limitations, while smoke and fog can degrade the operations of some systems. The clouds present a more serious problem because the radiations emitted can be enough to prevent the operations of the system itself.

Clouds also telltale the infrared radiation of the objects being targeted by the system.

ELECTROMAGNETIC

The electromagnetic signatures are caused by electronic radiation of communication and non-communication emitters. In other words, the detection of specific electromagnetic signatures can disclose the present of an activity in the area. This allows us to direct our sensors to that area in order to detect other signatures.

The communication signatures are generally direct -- use a radio and a signature will be provided. The battalions have certain communication systems; the brigades have other communication systems, and the elements of higher echelons also have different communication elements and other additional systems. To find the bigger units, to which a transmitter belongs, it is the duty to:

-- detect other transmitters in the area.

-- Use radio-goniometry to determine the location.

-- Categorize signals by a signal analysis.

-- Locate the type of transmitter in the vicinity of the area.

From this type of information, the intelligence can determine the location of a unit or command, supply point, weapons units, and assembly areas. This is particularly true when some radios or radars are used exclusively by a specific unit or weapons system. The movement, information of the order of battle, the structure of the radio network, tactical deployment, and, in a lesser degree, the intentions could be derived from the interception of the communications systems. All these could be detected and identified by knowing the location of communication equipment, without reading the messages.

The signatures produced by radars are considered from two viewpoints. First, when radar systems are activated they transmit signals and create signatures.

This makes our forces vulnerable when we use radar against the enemy. Secondly, the equipment, buildings and mountains have identifiable characteristics which the radar can be used to detect and identify. Therefore, the forces exposed are vulnerable to the detection by radar.

The military equipment have a great number of protuberances, angles and corners which the radar could detect. This refers to what is called the radar cross-section (RCS). Modern radar surveillance equipment can do more than solely detect the RCS of a target. Aerial radars with lateral view (SLAR) have enough resolution to identify certain weapons systems by detailed imagery or by its pattern. The radar systems can penetrate the fog, cloud and moderate rain. The surveillance radars are active systems and can operate against mobile or fixed targets.

The radar systems are limited in that they require an uninterrupted passage, or visibility points, towards the target area. However, have in mind that these systems cannot penetrate forests or heavy rain. The radar systems are susceptible to enemy interception and can become targets because of their distinctive signature.

PATTERNS

A pattern is the manner in which we do things. Patterns that can be predicted are developed by commanders, planners and operators. The different classes of patterns are as numerous as the different procedures in military operations. Some examples of patterns are:

- Command and Operations Posts
- Artillery fire before an attack
- Command posts located in the same position relative to the location of the combat units.
- Reconnaissance patrols repeatedly on a zone before an operation.

The officers need to examine their operations and activities in their zones of responsibility and reduce the established patterns whenever possible.

PROFILES

The profiles are a result of the actions taken by military units and individual soldiers. The profile analysis of a unit could reveal signatures and patterns on the procedures, and, eventually, the intentions of the unit could be determined. collectively, the profiles could be used by the enemy to find out our various courses of action. Our counterintelligence units develop profiles of our units in order to determine our vulnerabilities and thus recommend the commanders on the correction measures. In order to achieve this, all activity of the unit has to be identified to see if it presents indicators to the enemy.

Usually, profiles are developed by means of the gathering of information on the electromagnetic equipment and on physical actions and deployments.

Electromagnetic information identifies the activities of the units by associating the different signals with the equipment. Physical actions and deployments are things that the unit does: how a unit appears while it is performing; how it moves; its configuration during march or when it deploys. These different factors identify the different units.

In the majority of units, the electromagnetic and physical information is applicable to 5 areas of importance in order to complete an entire profile. The five profiles are:

-- Communications and command post

-- Intelligence

-- Operations and maneuvers

-- Logistics

-- Administration and other support

COMMUNICATIONS AND COMMAND POST

Some factors to be considered when developing and profile:

Where are the command posts located with regard to other units - particularly subordinate units?

-- How does the command post look like?

-- When is it transferred with regard to the other command elements?

-- Is the post surrounded by antennas - thus creating a very visible target?

-- What type of communications equipment is used and where is it located?

-- What is the amount of communications traffic with regard to the activities and operations?

-- Are there any road signs that might help the enemy units or agents to located the command post?

-- Do the logistics and administration communications compromised the operation?

INTELLIGENCE

Profiles on intelligence, surveillance, reconnaissance and elements identifying targets are developed in order to determine whether our activities indicate our intentions. Some considerations:

-- How frequently and to which zones have the land and air elements been assigned for information gathering?

-- Where are the information gathering elements located? (Which communication methods are used to report? Which are the information channels? Which are the security measures?)

-- How are the radars used? (For how long are they used before transferring them?)

-- Are there sensors in the target zone?

-- Have the reconnaissance vehicles (land and air) compromised the location of future operations?

-- Are the patrol levels been varied?

-- Can the different gathering activities relate to the different stages of operation - planning, preparation, execution?

OPERATIONS AND MANEUVERS

Activities during the preparation and execution of combat operations can be identified. Many activities are hard to cover due to the number of men involved, the noise, dust, tracks of vehicles, heat emitted, etc. However, the activities for combat operation have to be examined.

-- Can the drilling and instruction of men be easily detected?

-- If there is special training required for the operation, are there any special security measures?

-- Where are the units located before the operation? Artillery? Aviation? Reserves? Maintenance and supply? Is the movement indicated towards the front or the rear during their course of action?

-- How are the same actions carried out for preparation of offensive or defense operations? Do they indicate intentions?

LOGISTICS

Supply, maintenance, transportation and services and facilities indicating an operation have to be examined.

— Which movements indicate the starting of an operation?

— Are material and special equipment visible?

— Where is the material being stored? When?

— Is the change of schedule for vehicle and weapons maintenance indicating the start of an operation?

— Are new roads being built?

— Are special munitions being delivered secretly?

ADMINISTRATION AND OTHER SUPPORT

Activities seemingly completely innocent individually could provide valuable information for the enemy analyst. The administration and support profile could identify these actions which become obvious because they are different from what is normal. Some examples follow:

-- Things change before an operation:

  * Getting up and meals schedules?

  * Directions

  * Larger mail volume?

  * Frequency of reports:

  * Entry of licensed personnel?

-- There is a special request for:

  * Personnel?

  * Equipment?

  * Supplies of all types?

-- How is trash, paper, etc. being destroyed? Can enemy agents locate and use the waste?

-- Expecting wounded personnel by medical units, do they indicate a pending operation?

THE OPSEC PROCEDURE

1) To identify the enemy capability to gather intelligence (D-II/S-II).

2) Identify our EEFI and profiles.

Profiles + Patterns and signatures

Profile: All the characteristics pertaining a unit.

Patterns: Repeated activities established by SOP or by doctrine.

Signatures: Field actions of a unit.

-- visual
-- sound
-- infrared
-- electromagnetic

Profiles: Command Post

-- Communications
-- Operations
-- Logistics

3) Identify the vulnerable profiles that indicate our intentions.

4) Implement a risk analysis and make note of the EEFI.

```
-- Profiles      \
-- Patterns       > Indicators
-- Signature     /
```

5) Recommend OPSEC measures

-- Countersurveillance
-- countermeasures
-- Deception

6) Select the OPSEC measures.

7) Apply the OPSEC measures.

8) Apply efforts to monitor OPSEC.

9) Monitor the effectiveness of OPSEC.

10) Recommend OPSEC adjustments.

Step (1) --- OPSEC estimates

Step (2) --- OPSEC estimates

Step (3) --- Planning estimates/guidelines

Step (4) --- Estimate/guidelines

Step (5) --- Estimate/guidelines

Step (6) --- Estimate/guidelines

Step (7) --- OPSEC Annex

Step (8) --- OPSEC Annex

Step (9) --- OPSEC Annex

Step (10) --- OPSEC Annex

ESTIMATE --> GUIDELINE --> ANNEX

EVALUATION: YEARLY REPORT

OPSEC ANNEX

Item 1): Mission of the unit. (From the Plan of Operation)

Item 2): Summarize the enemy situation in terms of intelligence gathering, sabotage, and subversion. Discuss the situation with regard to recent enemy activities and their potential capability. This item is designed to indicate their capability for intelligence gathering; while item 3 include the measures to counteract those efforts. The following factors should be analyzed:

A. Indicate the effect of weather on the enemy's capability to gather intelligence on our OPSEC measures.

B. Indicate the effect of the terrain on the enemy's capability to gather intelligence on our OPSEC measures.

C. Resume the enemy's capability to gather intelligence and carry out sabotage and subversive actions. This includes:

1) Intelligence

A) Ground Observation and Reconnaissance

1) Eye observation
2) Patrols
3) Ground radars
4) Infrared surveillance
5) Long-range ground sensors
6) Other

B) Air Surveillance and Reconnaissance

1) Penetration flights
2) Long-distance flights
3) Reconnaissance satellites

C) Signal Intelligence

1) Communications Intelligence
2) Electronic Intelligence

D) Electronic Warfare

1) Interception and radio goniometry
2) Interruption
3) Destruction

E) Guerrilla, insurgents, agents

F) Other: infiltrators, refugees, prisoners of war, etc.

2) Sabotage

A) Military
B) Economic

3) Subversion
A) Propaganda
B) Terrorism
C) Political

D. Summarize the enemy's intelligence and security weaknesses. Summarize its intelligence gathering weaknesses, for committing sabotage and subversion sabotage. Discuss its internal security posture.

Item 3): Implementation

A: Make a list of all the countersurveillance measures taken by the field SOP. Emphasize new countersurveillance measures or changing of measures that are part of the SOP.

B. In this section, make a list of all the additional countermeasures that are not included in the SOP and are applicable to all the units. These countermeasures are designed to counteract a specific threat by the enemy counterintelligence.

Item 4): Miscellany

A. Summarize the threat to internal security. Discuss the problems of internal security detected in the command post.

B. Establish any special instructions not covered previously as targets of interest for counterintelligence (with priorities and locations).

C. Establish the chain of command for counterintelligence.

Item 5): Command

This item deals with instructions on where counterintelligence is sent to, the link between the various units, location of counterintelligence personnel, the different dissemination channels, types of reports required, frequency and priorities.

OPSEC ESTIMATION

Item 1): The Mission of the Unit. (From the Plan of Operations)

Item 2): Area of Operations. (Discuss the influence of the area of operations on the enemy capabilities to gather intelligence and commit acts of sabotage and subversion).

A. Time/weather. (From the Intelligence Annex)

-- The enemy's capabilities for surveillance and ground and air reconnaissance.

-- The time/weather is or is not favorable to the enemy's gathering efforts.

-- The impact of time/weather on our countermeasures.

B. Terrain. (From the Intelligence Annex)

-- Surveillance
-- Coverage
-- Natural and artificial obstacles
-- Key Terrain

(How the terrain affects the enemy's capability to gather information/intelligence and how it affects our countermeasures).

C. Other factors of the zone.

-- Political
-- Economic
-- Sociological
-- Psychological
-- Transportation

Item 3): Current Enemy situation on intelligence, sabotage and subversion activities.

A) Intelligence

1) Ground surveillance and reconnaissance.
-- Eye observation
-- Patrols
-- Ground radars
-- Infrared surveillance
-- Long-range ground sensors
-- Other

2) Air surveillance and reconnaissance
   - -- Penetration flights
   - -- Distance flights
   - -- Air Sensors
   - -- Reconnaissance satellites

3) Signal Intelligence
   - -- Communication intelligence
   - -- Electronic intelligence

4) Guerrillas and Insurgents

5) Espionage

6) Other: infiltrators
refugees, displaced persons,
prisoners of war, etc.

B) Sabotage

1) Military (installations, line of communication)
2) Economic

C) Subversion

1) Propaganda
2) Terrorism
3) Political

Item 4: <u>Enemy capability for intelligence gathering and to commit sabotage and subversive actions.</u>

A) <u>Intelligence</u>

1) Ground surveillance and reconnaissance.
   - -- Eye observation
   - -- Patrols
   - -- Ground radar
   - -- Infrared surveillance
   - -- Long-range ground sensors
   - -- Other

2) Air surveillance and reconnaissance
   - -- Penetration flights
   - -- Distance flights
   - -- Air Sensors
   - -- Reconnaissance satellites

3) Signal Intelligence

-- Communication intelligence
-- Electronic intelligence

4) Guerrillas and Insurgents

5) Espionage

6) Other: infiltrators
refugees, displaced persons,
prisoners of war, etc.

B) Sabotage

1) Military
2) Economic

C) Subversion

1) Propaganda
2) Terrorism
3) Political

Item 5): <u>Conclusions</u>

A) Indicate how the enemy will use its capability to gather intelligence and to commit sabotage and subversion actions.

B) Indicate the effects of the enemy capability on our course of action.

C) Indicate the effectiveness of our current countersurveillance measures.

D) Indicate the effectiveness of our current countermeasures.

E). Recommend additional countersurveillance measures.

F). Recommend additional countermeasures.

OPSEC PLANNING GUIDELINES

UNIT ______________________ COMMANDER: ____________________

G3/S2: ____________________ NAME OF OPSEC OFFICER: ______________

CONTENTS DISCUSSED WITH: ___________________________________
NAME RANK

PERSON COMPLETING REVISION: ________________________________

YES NO

CAMOUFLAGE

A.

B.

DOCUMENT SECURITY (INFORMATION)

A.

B.

COMMAND POST

A.

B.

COMSEC

SIGSEC

TRANSSEC

CHAPTER III

OPSEC EVALUATION

INTRODUCTION:

OPSEC means Operations Security. It is the duty of the Intelligence/ Counterintelligence Agent to determine the extent to which the security measures are being followed within the OPSEC program. If the measures have not been carried out, then nothing has been accomplished and the security of the command is in serious danger. When the OPSEC measures, developed from the OPSEC Procedures, are applied to an operation or activity (Commando) there are several methods to evaluate its effectiveness. All are included under the subject of "OPSEC Evaluation." The phrase OPSEC EVALUATION is applied to two different concepts:

a. One concept refers to an evaluation or study of the activity, unit, or project, using the OPSEC Procedure in order to recommend the OPSEC measures and create a Data base for Counterintelligence (CI).

b. The second concept is an evaluation of the effectiveness of the OPSEC measures already recommended. This evaluation might result in modification or suppression of measures, or the identification of new OPSEC measures.

OVERVIEW:

1. The OPSEC Evaluations vary, as already mentioned, depending on the units needs.

2. All evaluations have in common the characteristics of examining the effectiveness, the failure or the lack of OPSEC measures in a unit.

3. All evaluations are structured in a way that can provide complete and detailed information as to how the units and agencies are implementing the OPSEC measures.

4. THE OPSEC EVALUATIONS ARE NOT INSPECTIONS. The evaluations are presented and must be considered as <u>data finding</u> and/or <u>failure finding</u>.

5. The Evaluation is used to identify those areas of the security procedure of a unit that need to be improved.

6. When a team of agents carries out an OPSEC evaluation, it must be done sensibly and not overlook or ignore something, having always in mind that the evaluation results will be used to improve the system.

7. EVALUATIONS IN PEACE TIME AND IN WARTIME:

a. During peacetime the OPSEC Evaluations can be prepared several months in advance. An OPSEC evaluation of each command (unit) within a Division or Brigade, must be carried out annually.

b. In addition to a yearly evaluation, a commander may request it, through the G3/S3, that an OPSEC special evaluation be made of his unit.

c. During wartime, as vulnerabilities and threats are identified, the evaluations are carried out in response to an emergency request or urgency by the affected agencies.

8. Each evaluation is unique, since each one reflects the operation or activity being evaluated. However, there are certain common procedures for all evaluations, and these are as follows:

a. Planning
b. Evaluation
c. Report/Information

9. Planning of Evaluation:

The main factor in the planning stage of an evaluation is detail. It must be prepared in detail to carry out an evaluation. Normally, the planning stage includes the following:

a. Development of the purpose and scope of the evaluation:

The purpose/scope of the evaluation is prepared by the analysis section of CI, and by the OPSEC element, for approval by G3/S3.

SAMPLES OF POSSIBLE PURPOSES AND SCOPES OF AN EVALUATION:

(1) "This OPSEC Evaluation will discuss the vulnerability of the Division or Brigade to the multi-disciplinary threats of the enemy. These threats include Human Intelligence (HUMINT) and Signal Intelligence (SIGINT), etc.

b. <u>Selection of the team that will carry out the Evaluation:</u>

The team shall be selected by G3/S3, who will request its units to assign expert personnel in the areas of operations, intelligence, communications, logistics and administration. The team can be re-structured according to the type of evaluation to be made.

c. <u>Establish the contacts (link) in the area to be evaluated</u>:

One of the initial steps before evaluation is to contact the security chief of the installation to be evaluated. He can provide access to the necessary files needed for an evaluation.

d. Compilation of the reference materials:

The team must review the Standard Operations Procedures (SOP) of the unit to be evaluated. This will make the team familiar with the mission and the operational procedures of that installation.

e. Review the Essential Elements of Friendly Information (EEFI):

By reviewing the EEFI, the team may identify the valuable intelligence data which the commander deems important for the security of the installation. This information may include any information, classified or not, which, if revealed to enemy intelligence agent, could result in serious damage to the installation.

f. Review the threat of hostile intelligence:

The team must be familiar with possible espionage threats, activities of intelligence gathering by the enemy, by using all the sources in the area of operations.

g. Become familiar with the activity or installation to be evaluated:

Members of the evaluation team shall review all the directives of the installation. The evaluation team leader should be briefed by the commander of the installation.

h. Prepare organizational charts:

Preparation of organizational charts for evaluation purposes will facilitate the evaluator's work. The chart should be prepared according to the area to be evaluated. The charts should include the areas to be reviewed by the agents and specific notes that might be useful for the individual evaluator to carry out his duties.

i. Give notice of evaluation:

The final step in the preparation of an OPSEC evaluation is to notify it. The G3/S3 notifies the installations that will be evaluated by means of an amendment. The information that might appear in the message is as follows:

(1) The purpose and scope of the evaluation.
(2) The members of the evaluating team and its access to classified information.
(3) Necessary briefings and familiarity.
(4) Date and time that will be spent in the evaluation.
(5) Support required from Signal Security (SIGSEC)

10. The Evaluation:

After completing the planning stage, the evaluation will be performed. The following steps, in order, must be carried out at the onset of the evaluation.

a. Beginning briefing:

This briefing could be formal or informal. It must be given by the evaluating team leader. The areas to be covered during this briefing are:

(1) Purpose and scope of the evaluation.
(2) How the evaluation will be conducted.

(3) Summary of the enemy threats and the vulnerability of the installations to these threats.

(4) Previous OPSEC evaluations, if any, will be discussed.

b. Briefing by the Commander:

This briefing will give the Evaluating Team an opportunity to receive information on the operations from the viewpoint of the commander of the installation.

c. The Evaluation: (Information that will be covered later on by this chapter).

d. Final Briefing:

The purpose of the final briefing is to inform the Commander of the results of the evaluation and the findings during the evaluation with regard to the OPSEC system of his installation. Also, the outgoing briefing could be an informal one.

e. Report:

During this period, the evaluating team, the analysis section of CI and the OPSEC section, shall evaluate all the information obtained during the evaluation. The product of this effort shall provide a data base that can be used to identify the vulnerabilities of the installation in the OPSEC areas. The evaluation results of the information obtained by the team will be the basis for recommendations of new OPSEC measures, if necessary.

OPSEC EVALUATION

BROCHURE: TECHNIQUES AND AREAS TO BE COVERED DURING AN OPSEC EVALUATION.

OPSEC EVALUATION

HUMAN INTELLIGENCE

A. Security of Information:

1. Reproduction machines (copiers):

a. How many machines are there?

b. What is the control on the reproduction of classified material?

c. Who is authorized to reproduce classified material?

d. Who authorizes reproduction?

e. Has the personnel been instructed that when a document is copied in a copier, the image of the document remains latent in the crystal and could emerge if a blank paper goes through.

2. Destruction of classified information:

a. Who does the destruction of classified information?

b. Where is destruction carried out?

c. When and how often is classified information destroyed?

d. How is it destroyed?

e. What security measures exist during the destruction process of classified material?

3. Emergency Evacuation and Destruction Plan:

a. Obtain a copy of the plan and review it to determine whether it is effective:

b. How is the plan carried out?

c. Do they have the necessary materials on hand to implement the plan?

d. Has the plan been rehearsed (drilled)?

4. Sensitive unclassified Trash:

a. Is there a procedure with regard to the handling of sensitive unclassified trash?

b. Is there any mention of it in the SOP?

c. Is the SOP specification carried out?

d. How can they be sure that the command instructions are carried out with regard to sensitive unclassified material?

e. Is all the personnel aware of the importance of controlling the sensitive unclassified trash? How were they instructed?

5. Requests for information:

a. How are requests for information processed?

b. What is the procedure if the request originates from another military or civilian command, or foreign country?

c. How do they control publication of information on activities evaluated by other sources?

d. Is there an Officer for Public Relations (PRO)?

e. What are the responsibilities of the PRO in this program?

f. How is unsolicited mail handled?

6. Open Publications:

a. Which are the open publications of the installation? (A publication which is unclassified and anybody can have access to it.)

b. Obtain copies and determine whether the publication has any EEFI information.

c. How are open publications controlled?

7. EEFI:

a. Obtain copy of the current EEFI list.

b. On what was this list based?

c. Is all the necessary personnel aware of what is included in the EEFI list? Is this information denied to some personnel?

d. Is the EEFI list realistic, does it in fact contain everything that the unit wants to protect?

8. Reports of Previous Inspections/evaluations or Studies:

a. Obtain copies of all the inspections, evaluations, studies, of physical security, personnel, OPSEC, that has pertain to the installation.

b. Review all the reports and determined which measures have been taken to correct problems identified previously.

9. Special Access Material:

a. Which materials requiring special access are used by the installation?

b. What security measures are enforces to protect and safeguard the material?

10. Classification guidelines:

a. Obtain copy of the classification guidelines for classified material of the installation.

b. Are these guidelines effective?

c. Are they written in an efficient way, providing the necessary information?

d. Is the personnel knowledgeable of this classification guideline?

11. Casual Conversation.

a. During the evaluation of the installation, try to listen to conversation carried out in areas where classified or sensitive matters should not be discussed; also be on the alert to conversation between persons that have access and the need to know certain information with persons that do not have the need to know nor the access.

b. Which is the procedure of the unit/installation regarding casual conversation?

c. Does the installation have an instruction program to brief its personnel with regard to the danger of casual conversation?

12. Security Education Program:

a. Which is the level of security education of the evaluated installation?

b. Is there an education program in the areas of sabotage and espionage against the armed forces, OPSEC, SigSec, Humint, and imagery intelligence?

c. If there is a program, is it effective? (Does the personnel respond to the teachings?)

d. Has the installation informed on any attempt of sabotage and espionage or incident to the SEAAF?

e. Is the personnel contacted aware of the purpose of OPSEC? Could they identify an approach to SEAAF if it would happen to them?

B. Physical Security

1. Inspections after working hours:

a. Are inspections of the installation carried out after working hours?

b. If they do, what do they look for?

c. How often are these inspections performed?

d. What happens if they find loose classified material or any other security violation?

2. Effectiveness of Physical Security:

a. What is the concrete effectiveness of the physical security of the installation?

b. Are the current physical security measures adequate?

c. Examine doors, gates, fences, barriers, etc. and determine its weakness and strong points.

3. Inspection Program of the Security Inspector:

a. Does the installation have an inspection program by the Security Supervisor?

b. When the security supervisor carries out an inspection, is it announced or unannounced?

c. Is the personnel performing the physical security inspection, assigned to the same installation which they are inspecting?

d. What do they look for when inspecting?

e. What happens when they discover a vulnerability?

4. Access Control:

a. Pretend you are a hostile intelligence agent and determine how could you manage to enter the installation. Plan it from the outside to the inside and how far could you penetrate. Try to obtain classified material or try to listen to casual classified conversation. Use your imagination. The enemy will do the same.

b. Are the gates adequate?

c. Is there a cleared zone beyond the perimetry fences?

d. Is there an adequate number of guards? Are they duly trained? (How do they communicate among themselves?

e. Are the fences adequate?

f. Are the outer doors adequate?

g. Is the alarm system adequate? (Do they have an alarm system?)

h. Is there a control of visitors and their vehicles?

i. Do the guards have an established routine of movement that will make them vulnerable to an attack?

j. Is there a reserve/support group that could assist in case of a surprise attack?

k. Prepare a scenario of how you could penetrate the installation, include a detailed account of the weak and strong points of the security program of the installation.

5. Pass system:

a. Is it adequate?

b. Can the passes be reproduced easily?

c. Is there another system that could be used in case the first one is compromised?

d. How are passes destroyed?

e. What happens when they are informed that a pass has been lost?

f. Do they allow for one pass to have access to the entire installation, or are there restrictions?

g. If the pass is not shown, is he made aware by the other individuals, or is he allowed to walk without problem or question?

h. Are all the passes always visible?

i. How is the access to classified information certified or verified of an individual visiting the installation?

j. Are visitors escorted through the installation?

k. Is there a record of the passes?

l. How many times a year is the pass system changed?

6. Visitors control:

a. What kind of access is authorized to visitors?

b. How are their level of access to classified information verified?

c. Are the visitors required to sign at the entrance? What information are they required to provide?

d. What other controls are applied for visitors?

7. Foreign Liaison Visitors

a. Are their access or authority for visiting verified?

b. Who is notified of their visit to the installation?

c. Which areas are they allowed to access?

d. What type of information is exchanged?

e. Is a briefing offered to the personnel that will have contact with the foreign visitors?

8. OPSEC Support - Physical Security Plan:

a. Review and determine whether the plan is effective,.

b. Does this plan provide the support/information/guidelines needed?

c. Can a Study of Physical Security be carried out?

d. What do the personnel know of the Physical Security Plan?

e. Is it reviewed and updated frequently?

9. Instructions for the Guards

a. Are the instructions to guards adequate?

b. Do the instructions to guards indicate which are their responsibilities?

c. Are emergency plans included in the instructions?

d. What do the guards know about the plan?

e. Do the instructions include how to proceed in case of a bomb threat, sabotage, espionage, events of interest for the CI, and the destruction of government property?

f. Do the guards understand what they have to do if they are involved in an incident that concerns the military intelligence?

C. Personnel Security

1. Human Reliability Program: (This program is used to determine the reliability of persons in sensitive posts. The subject is discussed in the Chapter entitled "Security Investigation of Personnel")

a. Does the installation have such a program?

b. If it does, how is it checked?

c. What has this program offered to the Commander?

d. How is access to classified information validated?

e. Where do personnel whose access has not been approved yet work?

2. Travel Abroad by Staff Personnel:

a. Where to and when do these individuals travel to foreign countries?

b. What is the procedure to notify the commander of these trips?

c. Are the travel schedules controlled/evaluated?

d. Is the personnel travelling abroad briefed?

e. What kind of information do they carry and what kind of information can they exchange?

f. Are trips abroad reported to military intelligence?

3. List of Accesses to Classified Information:

a. Is there a list of all the persons who have access to classified information?

b. Do the personnel have access to the necessary information to carry out their tasks?

c. Revise the access list and determine whether there is any individual with access to information who should not be allowed.

d. How does the command verify the access to classified information of other agencies?

4. OPSEC Program:

OPSEC SOP:

a. Does the installation have an OPSEC SOP?

b. Is it adequate?

c. Does the SOP of OPSEC describe the responsibilities of everybody down to the individual level?

OPSEC Officer

a. Does the officer in charge of OPSEC working full-time for OPSEC, or does he have other primary functions?

b. Which are the responsibilities of the OPSEC officer?

c. What kind of support is given to him?

d. Does he have the experience/education/reference material necessary to carry out his tasks?

e. What importance does the Commander bestow on the OPSEC program?

OPSEC Analyst

a. Is the command aware of what is an OPSEC analyst?

b. Does the command know what an Analyst can do for them?

c. Have they requested support by the OPSEC Analyst, and what kind of support was requested?

d. Have they received in the past any support by an OPSEC Analyst?

e. Is the OPSEC Analyst effective?

4. OPSEC Consciousness:

a. Does the personnel know what OPSEC means, what OPSEC can do for them to protect their mission and work material?

b. Is OPSEC considered a daily routine in this installation?

c. Is OPSEC considered before, after and during a military exercise?

d. What kind of OPSEC training have been given to the personnel?

e. Does the personnel believe in the importance of OPSEC?

f. Which is your (the agent's) opinion of the total consciousness of OPSEC in the installation?

D. <u>Signal Intelligence</u>

1. SOP:

a. Obtain and review all the SOP's of SIGSEC. (are they adequate?)

b. Are they reviewed and updated periodically?

2. Support by Signal Intelligence:

a. What kind of support has the installation received from Signal Intelligence?

b. What kind of signal intelligence support does the installation need?

3. Safe Communication:

a. What are the means for safe communication?

b. Are they adequate?

c. Is there a backup system in case the primary one stops working?

4. Inspections of Safe Communications and Signal Security:

a. When was the last SIGSEC/COMSEC inspection done and what were the results?

b. Does the system need to be improved? (Were the improvement measures carried out?)

c. Is there a need currently to improve the SIGSEC and COMSEC systems?

5. Security Education:

a. Is the installation personnel trained on communications security?

b. If they are trained, how is instruction given, is it accepted or rejected?

c. Is there a need to improve the security education program?

6. ADP Security:

(ADP: is a security system used to protect the computer communication)

a. Is the personnel trained on COMSEC?

b. Is a key code used? How can an unauthorized person be prevented to access the computer system?

c. Do unauthorized persons use the system?

d. What is the software used? What classification does it have?

e. What is the procedure for controlling the computer output?

f. What physical security measures are used to protect the computer terminals that are outside the computer room?

g. Which procedure is used for the necessary maintenance?

h. If the system contains classified information, how can they get the cleared personnel to carry out the computer maintenance?

i. Is there a Security Officer assigned for the computer room?

j. Are the computer operators trained on the need to protect the systems security?

k. Can classified information be obtained through the terminals?

l. Are visitors escorted while visiting the computers area?

m. Is there a pass system for the computers area?

n. Does the installation share the use of computers with other installations or agencies?

E. Imagery Intelligence

1. Aerial Photography:

a. Is the personnel conscious of the existence/threat of aerial photography?

b. Is the installation vulnerable to this threat?

c. What precautions are taken for protection against this threat?

d. What kind of written information do they have to protect themselves against this threat?

2. Manual Photography by an Agent:

a. Is the personnel conscious of this kind of threat?

b. What physical security precautions are taken to protect themselves against this threat?

c. How vulnerable is the installation?

d. Are the guards aware of this threat and know how to prevent it?

3. Outside Tryouts

a. Does the installation conduct tryouts outside the building that could be vulnerable to the threat of imagery intelligence?

b. Has the command considered using camouflage before the tryouts are carried out?

c. Does the SOP contain something with regard to the protection against this threat?

F. <u>Vulnerabilities/Recommendations of Signal Intelligence</u>

G. <u>Imagery Intelligence</u>

1. Local threat:

2. Vulnerabilities/Recommendations:

H. <u>Other Vulnerabilities and recommendations as appropriate</u>:

I. <u>Remarks</u>:

(General remarks are included which are not qualified as vulnerabilities.)

J. <u>Conclusions</u>

(Support to be given to the installation in the future.)

I. ANNEXES:

a. Data on Threats in general.

b. Results of the COMSEC evaluation.

c. Study of Signal Security

d. Essential Elements of the Enemy

e. Report of ADP Security

f. EEFI - Evaluation

g. Inspection of Technical Support

h. Other information or reports that might backup the OPSEC Evaluation.

NOTE: Not all the Annexes mentioned above are required in all the reports of an OPSEC evaluation.

CHAPTER IV

DOCUMENTS SECURITY

INTRODUCTION:

The application of this chapter will be based on the following main principles:

1. It is essential that some official information be given top protection in order to safeguard the capability of the nation to protect itself against all hostile and destructive actions.

2. It is also essential that the citizens of the nation be informed as much as possible on the activities of the government.

3. This chapter should not be interpreted in any way as trying to withhold information that otherwise could be publicly disseminated.

GENERAL:

A. DEFINITION OF DOCUMENT SECURITY: The degree of protection given to certain official information for the safekeeping of the nation's capability to protect itself against hostile or destructive actions.

B. All personnel must be aware that the above-mentioned principles are the fundamental factors that govern military security and must be deeply indoctrinated so as to be inherent with the routine performance of their tasks.

C. ORGANIZATION:

1. Categories of Classification

a. The official information requiring protection in the interest of national defense will be limited to three categories of classification, which are, in order of importance, TOP SECRET, SECRET and CONFIDENTIAL. No other designations shall be used to classify information of national defense.

2. Other Definitions

a. Information of Defense. It pertains the official information that requires protection in the interest of national defense that is not of common knowledge, y which could be valuable military information for a potential enemy, to plan or sustain war or insurgency against us or our allies.

b. Classified Material. It is the official information which has been classified and marked with one of the categories mentioned above.

c. Access to Classified Material. It allows access to classified material only to those persons authorized to work with classified information and need to know such information to be able to accomplish their official duties.

d. Custody. Is the person in possession or that has the responsibility of protecting and accounting for classified material.

e. Inventory. It is the procedure used to account for classified material by control of entry and record of the document, or entry of destruction record, or by signed receipts.

f. Document. Is any recorded information, without considering its form or characteristics, and includes, without being limited to, the following:

(1) Handwritten, typewritten or printed material.

(2) All drawn, painted or engraved material.

(3) All sound recordings, voices, tapes or records.

(4) All types of photographs and films, in negatives or processed, fixed or in motion.

g. Authority for Derived Classification: It is the authority to classify material as a result of being connected to, or in response to other material related to the same subject of an already classified material.

h. Material: Means any document, product or substance, on or within which information can be recorded or included.

i. Properly authorized person: It is a person who has been authorized to work with classified information, according to the established norms.

3. TOP SECRET Information. Top Secret classification is limited to the information of defense or material that require the highest degree of protection. TOP SECRET information will be applicable only to that kind of information or material that is extremely important for defense, and the unauthorized disclosure of which would result in serious danger for the nation, as for example:

a. Definite severance of diplomatic relationships, that would damage the defense of the nation; [leading] to an armed attack against them or their allies or to a war.

b. Compromise the military defense plans, or the operations of military intelligence, or technical or scientific developments vital for the national defense.

c. As examples of this type of information, there are:

(1) A strategic plan that documents the complete operations of war.

(2) The documents for war planning.

(3) Plan of operations for an independent operation, or for a series of coordinated operations.

(4) Documents of military intelligence containing complete information of a nature that would reveal a big effort of military intelligence activities by the nation, and that would enable unauthorized persons to evaluate the success obtained by the military intelligence services of the nation.

(5) Plans or programs to carry out operations of military intelligence, or other special operations, when the knowledge of a particular plan, program or operation would result extremely damaging for the nation.

(6) Important information regarding equipment (war materiel) extremely important and radically new, whose technical development constitute vital information for the defense of the nation.

4. SECRET Information. The use of SECRET classification will be limited to defense or material information whose unauthorized dissemination could result in serious damage for the nation, such as:

a. Jeopardize international relations of the country.

b. Endanger the effectiveness of a program or policy vitally important for the national defense.

c. Compromises important military plans for the defense or the technical development for the national defense.

d. Reveals important operations of military intelligence.

e. Examples of this type of information are:

(1) A war plan or a complete plan for a future war operation not included under the TOP SECRET classification, and documents that indicate the disposition of our forces, whose unauthorized publication, by itself, could compromise such secret plans.

(2) Defense plans and other military plans not included under the TOP SECRET classification, or in the previous paragraph, that contain plans and development programs or acquisitions, although they do not necessary include all the emergency plans.

(3) Specific intelligence that, by itself, could reveal the military capability of degree of preparation of the Armed Forces, but does not include information whose unauthorized disclosure could compromise a TOP SECRET plan.

(4) Intelligence that reveals the strength of our forces involved in war operations; quantity or quality of equipment, or the quantity or composition of the units in a theater of operations or other geographic area where our forces might be involved in war operations. During peacetime, the information that would reveal the strength, identify, composition or situation of units usually would not require SECRET classification.

(5) Military intelligence or other information whose value depends on concealing the fact that the nations possesses it.

(6) Details or specific information related to new material, or modification of material that reveal important military advances, or new technical development that has direct application of vital importance for the national defense.

(7) Security measure for communication or cryptographic material that reveals vitally important information for the national defense.

(8) Intelligence of vital importance for the national defense, with regard to amounts of war reserves.

f. <u>CONFIDENTIAL INFORMATION</u>. The use of CONFIDENTIAL classification will be limited to defense information and to the material whose unauthorized disclosure could be damaging to the interests of the national defense. As examples of this type of material, there are:

(1) Reports of operations and battles that might have valuable information for the enemy (The Essential Elements of Friendly Information).

(2) Reports that contain military intelligence, no matter what type of information.

(3) Frequencies of military radios and call signals that have special meaning assigned, or those that are frequently changed because of security reasons.

(4) Devices and material related to the communications security.

(5) Information that indicates the assets of our ground, sea and air forces in national territory or abroad, or the composition of the units, or que quantity of specific equipment units that belong to them. During peace time a defense classification is not necessary unless such information reflects the numbers of the total assets or quantity of weapons whose characteristics are themselves classified.

(6) The documents or manuals that contain technical information used for training, maintenance or inspection of classified war material.

(7) Doctrine of tactical or technical operations.

(8) The investigation, development, production and acquisition of war materiel.

f. Handling of classified documents

(1) Protection of classified material in the hands of persons that are travelling.

(a) A person receiving travel orders, and who is authorized to carry classified material, will protect such material by the following methods:

1- He will contact his commander in order to obtain, if available, the corresponding means of protection, according to the particular classification of the material, or;

2- Will keep the material under his personal control continuously. It is the responsibility of the carrier of classified material to use his best judgement for his actions, in order to avoid risky situations that might compromise the classified material.

(b) The personnel on travel mission will not carry classified material when crossing international borders where the classified material might be subject to scrutiny by Customs inspectors or other "unauthorized" persons. Such material, when forwarded previously by diplomatic pouch or by mail, will not encounter any obstacles on its way.

(2) Covers of classified material.

The cover of classified material is used to call the attention of the personnel handling it, to the fact that it is a classified document, and to protect it against unauthorized scrutiny. The cover shall have the stamp identifying the classification of the document.

(3) Destruction in case of emergency.

(a) Plans

The commanders and chiefs that are responsible for the protection of classified material will make formal plans for the destruction or safe transfer of all classified material under its jurisdiction, in case of civilian disturbance, disaster, or enemy action.

(b) On board aircraft or ships

If the aircraft carrying classified material is forced to land, or a ship runs aground in unfriendly or neutral territory where capture seems imminent, or in other circumstances when it appears that the material should be destroyed so as not to be recognized, it is preferable to burn it or destroy it in a way that will not be recognizable.

(4) Security of the typewriter ribbons: The typewriter ribbons, whether made of cotton, rayon, paper, or silk, which are used to write classified information are not safe until they have been written over twice. Presently, many of the ribbons for typewriter machines can only be used once, therefore have in mind that the impression of letters remain in the ribbons and these are significantly valuable for the enemy as is the paper in which the information was typed. These ribbons should be protected accordingly.

(5) Classified trash: Trash such as drafts, minutes, notes, dictaphone recordings, or other recordings, typewriter ribbons, carbon paper, rolls of film, and similar articles, containing information of national defense, shall be protected by a responsible person, according to their classification, until they can be destroyed in an orderly fashion the same as for material of similar classification. It is necessary to have a certificate of destruction.

CHAPTER V

LIAISON

INTRODUCTION:

The purpose of this chapter is to enable you to plan and carry out Liaison with Government and civilian Agencies for collection of information/ intelligence required, in compliance with the commanders requirements, without losing a mutual confidence with the Source.

GENERAL:

A. Before carrying out a Liaison, it has to be determined first which agency or source will be contacted and the purpose for the contact:

1. Liaison could be carried out with the following sources or agencies:

a. Government agencies
b. Military units or agencies
c. Civilian agencies and industry

2. The purposes for carrying out the liaison are:

a. To establish a relationship of mutual confidence between the various government agencies.

b. To develop sources of information for immediate or future exploitation.

c. To collect and exchange information that might be useful for future investigation.

d. To obtain assistance in investigations or CI operations.

B. With this in mind, there are two forms or types of Liaison that can be carried out:

<u>FORMAL LIAISON and INFORMAL LIAISON</u>

1. Formal liaison is carried out to obtain:

a. Specific information for an ongoing investigation.

b. Information related to security violations.

c. Information of threats to the national security.

2. Informal Liaison is carried out to:

a. Establish a relationship of mutual confidence.

b. Develop Sources.

c. Obtain information related to specific investigations.

d. Obtain information that has not been requested specifically but is related to one or more incidents or investigations.

e. Maintain friendly relationship among the Sources of information and the CI agents.

C. Before starting a liaison, you should review the SOP of the unit to determine the proper Liaison procedure in your area of operations.

D. Upon reviewing the SOP you should determine the requirements and establish priorities according to the SOP. Some of these areas are:

1. The priority of intelligence requirements are selected by the Commander, higher authority or by the mission.

2. The requirements are generated by the direction taken by the investigation.

3. The priorities that have been established based on the recommendations by the Commander or the urgency of the mission.

E. Once the requirements have been reviewed, you can establish the liaison contact.

1. There are three basic methods to establish a contact, and these are:

a. Personal Approach: This is done by the person (Agent) actually carrying out the liaison with the Source. This individual (Agent) introduces personally the new Agent to the Source. This method is preferred because it has the advantage of transferring the credibility and confidence of the old Agent directly to the new Agent or contact.

b. Introductory letter: In this method the new Agent obtains a letter of introduction from a person or old Agent that knows the Source. This letter is presented to the Source during the first contact. The other method of introduction letter is to send a letter to the Source indicating that you wish to visit him.

c. Cold Approach. This is the least effective method since it involved making the initial contact with a strange person. The first visit of this approach should always be on a social level and must be a short one.

2. When you have not done any personal contact with the Source, you must take into consideration the following:

a. The Agent must introduce himself and present his official credentials identifying him as a Special Agent of Officer of Military Intelligence.

b. Indicate the purpose of the visit.

c. Based on your personal observation of the Source's reaction, determine if a casual conversation is appropriate.

d. As the Agent you must be alert all the time to the signals by the Source that might indicate what kind of approach is better to use with the Source.

e. The Agent must be cordial, professional and sincere.

f. Must show respect for the position or profession of the Source.

3. If there has been a previous personal contact with the Source, the actions of the Agent could be more relaxed (calm) according to the relationship established by previous contacts.

F. During the liaison, you must establish a Relationship of Mutual Confidence in order to:

1. Establish cooperation between you and the Source. A great deal of precaution should be used to develop the Source's willingness to cooperate, because you do not want to compromise the Source.

2. Have in mind that you can obtain information from previous liaison reports and other documentation that may assist you in determining the type of approach that would be best for the Source in particular in order to:

a. Adopt the proper attitude.

b. Be ready to change attitude if it is necessary. As the Source calms down and starts to cooperate, a more relaxed attitude could be helpful.

3. One of the techniques that you can use is to deal with subjects of mutual interest.

EXAMPLE: "If a person is a football fanatic, he would very receptive to talk about that sport instead of another sport that he does not know, or does not care to about."

4. During the liaison contact you must show sincere interest in the Source's opinions. If the Agent shows that his (Agent's) opinion is better than the Source's, you might lose the Source's confidence.

5. It is important, also, that you study well the capabilities of the Source before asking him for information. This might embarrass the Source if a request is made that he cannot fulfill.

6. You must always be aware of the jealousy existing among the various Agencies. And remember always that you do not have to compare the effectiveness of one Agency against the other, this could cause a serious problem because the Source could also be providing information to other agencies where you might also have another contact.

7. During the Liaison contact, maintain always your position as a CI Special Agent and do not fall into discussion of military ranking; this is very important because you are a direct representative of the government.

8. If you do not have any previous knowledge of the Source, establish the contact and mutual confidence in the manner already discussed. In this situation, maintain flexibility and allow the circumstances to dictate on the approach that can be used with the Source.

G. During the liaison contact there will be instances when information of mutual interest will be exchanged.

1. Before exchanging such information, first determine if that information can be divulged. Consider the following points as basis for such exchange:

a. Whether the information does not violate the SOP stipulations.

b. Whether it is classified and cannot be divulged among other agencies, even if they are part of the Government.

NOTE: The exchange of information is important because if you only obtain information and does not offer certain information in return there is the possibility of losing the Source's confidence.

2. The Liaison contact can be considered successful when:

a. both parts involved in the Liaison decide or discuss the exchange of information.

b. both parts can use the information exchanged to their advantage.

CHAPTER VI

PREPARATION OF THE LIAISON REPORT

INTRODUCTION:

Upon conclusion of a liaison contact, a report of the liaison has to be prepare to include all the identification data of the Source; all the information on previous contact reports; a description of the circumstances of the contact and operational matters; data of the Source's background; a list of all the other reports prepared in relation to this contact; all the information related to the financial and logistic support, remarks (if applicable) and the signature of the Agent.

GENERAL:

A. First determine whether the liaison report is necessary or allowed/authorized (Some countries prohibit the documentation of information by the citizens of the same country).

1. Prepare the liaison report after the contact has been completed.

B. Complete the heading of the report (See Figure No. 1)

1. TOPIC/SUBJECT: Write down the name, position, organization, and other data that identifies the Source, as requested by the local SOP. If a code number has been assigned to the Source, use only this number for identification.

2. REFERENCES:

a. Write the date and control number of the last Liaison Report prepared in regard to this Source.

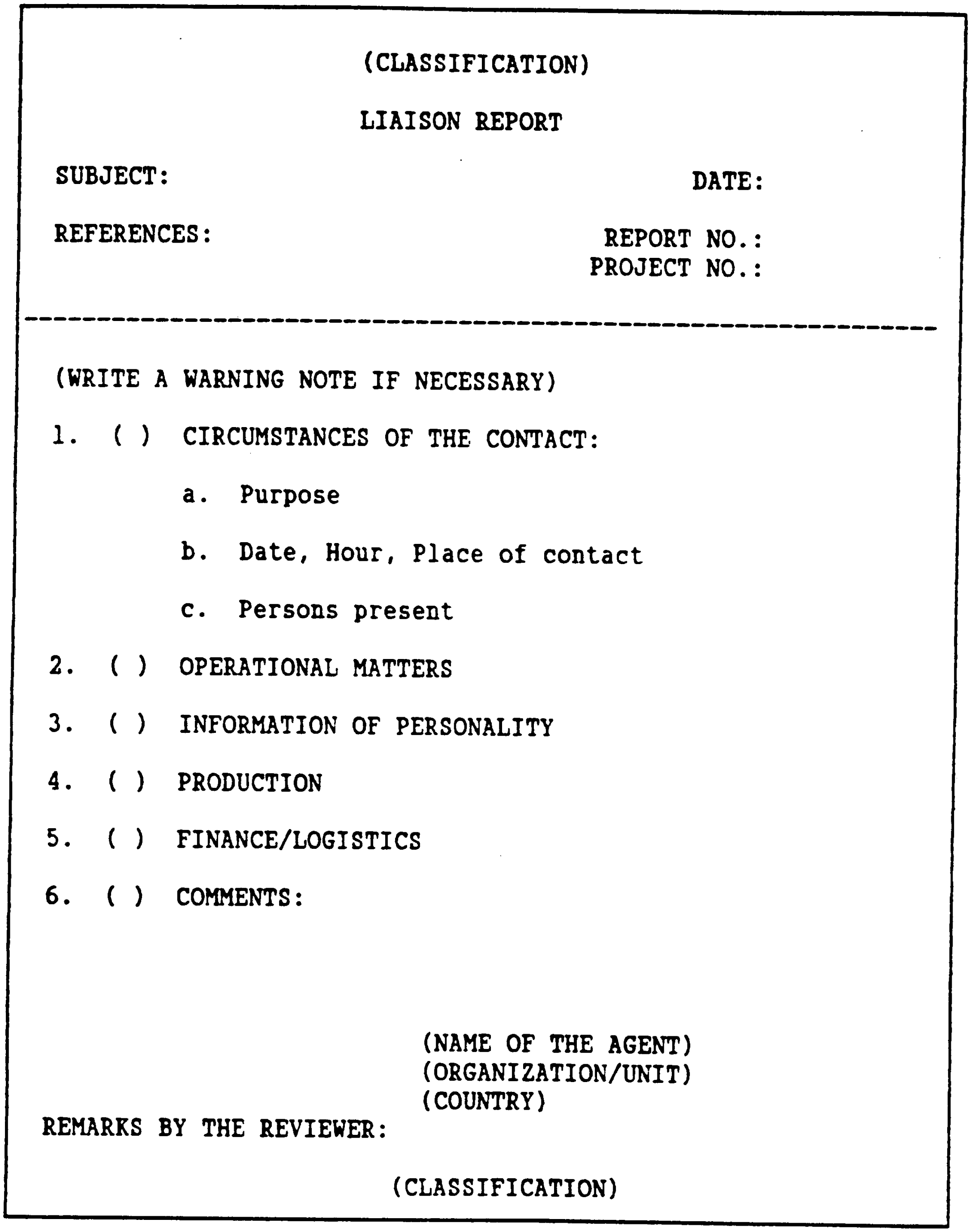
b. If there are no previous reports on this Source, make a note of it in the Report you are preparing.

c. Note down all the documents and material that were originated by, or related to, the Source.

3. DATE: Note down the date of preparation of the report.

4. NUMBER OF THE REPORT: Write down the number of the report, it depends on the SOP of the unit. Usually, the CI section keeps a record of all the sequential numbers used for Liaison Reports.

Figure #1



(CLASSIFICATION)

LIAISON REPORT

SUBJECT: DATE:

REFERENCES: REPORT NO.:
PROJECT NO.:

(WRITE A WARNING NOTE IF NECESSARY)

1. ( ) CIRCUMSTANCES OF THE CONTACT:

   a. Purpose

   b. Date, Hour, Place of contact

   c. Persons present

2. ( ) OPERATIONAL MATTERS

3. ( ) INFORMATION OF PERSONALITY

4. ( ) PRODUCTION

5. ( ) FINANCE/LOGISTICS

6. ( ) COMMENTS:

(NAME OF THE AGENT)
(ORGANIZATION/UNIT)
(COUNTRY)

REMARKS BY THE REVIEWER:

(CLASSIFICATION)

5. NUMBER OF THE PROJECT: In the CI cases, usually, each investigation or project has a number assigned to it. The unit's SOP assigns those numbers if applicable.

C. WARNING NOTE: If necessary, include in this section of the Report a note that will indicate the sensitivity of the investigation or the contact, as shown in the following example:

"WARNING: SOURCES AND SENSITIVE METHODS INVOLVED"

D. COMPLETE PARAGRAPH #1: "CIRCUMSTANCES OF THE CONTACT" (SEE FIG.#1)

Describe the circumstances of the contact including:

1. Purpose

2. Date, hour: use the expression: "from ... to ... of May 19.."

3. Place where the contact occurred.

4. Persons present: Whether there were other persons present during the contact, note down their complete physical description and other pertinent details.

E. COMPLETE PARAGRAPH #2 (OPERATIONAL MATTERS)

1. List in chronological order all the events and subjects discussed during the contact.

2. Mention briefly any operational information that has not been included in other reports.

3. Write down all additional information and the identification of new leads or Sources with as much detail as possible.

F. COMPLETE PARAGRAPH #3 (INFORMATION OF PERSONALITY)

Give information related to the Source as completely as possible. This will include, but not limited to, the following:

1. Personality or personality traits.

2. Idiôsyncracies, peculiarities of the Source.

3. Sense of humor, or lack of it.

4. Type of information that the Source is willing to discuss.

5. Topics that must be pursued or disregarded.

6. Background information on the Source that has not been reported before.

NOTE: If a code number has been used to identify a Source in this report do not give information of personality that might compromise or identify the Source.

G. COMPLETE PARAGRAPH #4 (PRODUCTION):

List, according to the report's number, all the documents that were produced as a consequence of the contact with the Source.

H. COMPLETE PARAGRAPH #5 (FINANCES AND LOGISTICS): If applicable, include a list of:

1. Incentives used
2. Amount of expenses:
   a. Official funds
   b. Personal funds

I. COMPLETE PARAGRAPH #6 (COMMENTS)

1. Write down comments that the Agent believes are applicable but cannot be confirmed (personal opinions, intuition, etc.)

EXAMPLE: "During this contact the Source appeared to be very nervous. In previous contacts the Source never showed to be nervous."

2. Explain the specific purpose of all the expenses paid in cash by the Agent, disregarding "when", "where" or "why."

J. FILL OUT THE SIGNATURE BLOCK

1. Name of the Agent
2. Official title or position
3. Office to which Agent belongs
4. Country where the Agent's office is located

K. CLASSIFY THE REPORT

L. PREPARE THE REPORT IN TWO COPIES:

1. Sign both copies
2. Forward one copy to the Higher Control Office
3. Keep a copy for your office files.

CHAPTER VII

INTRODUCTION - INVESTIGATION OF PERSONNEL SECURITY

INTRODUCTION

A definite concept with regard to security is that no person, merely because of rank or position, has the right to know or possess classified information or material; and that such material will be entrusted only to those individuals whose official or governmental functions require knowledge; and that all persona that require access must be authorized to received classified information or material. These individuals must be of undisputable loyalty, integrity and discretion; must posses excellent character and have such habits and associations that leave no doubt at all of its good judgement in the handling of classified information and material.

GENERAL:

A. SECURITY is the responsibility of the Command:

1. The Commanders may delegate work and functions, but responsibility cannot be delegated. One of the most important functions of Military Intelligence is to assist the commander is establishing and maintaining security. The Investigation of Personnel Security (IPS) is one of the methods used to attain that security. The investigation is done of the individuals occupying sensitive positions and are under the jurisdiction of the military service, or of individuals considered for filling out positions of confidence that require access to classified information or materials.

B. SENSITIVE POSITION

1. A sensitive position is any post within the military services whose occupant could cause an adverse effect to national security by virtue of the nature of his responsibility.

2. All sensitive positions require an Investigation of Personnel Security (IPS)

a. Any positions whose functions or responsibilities require access to classified defense material.

b. Functions related to classified systems and cryptographic equipment.

c. Functions related to studies and investigations and/or classified development.

d. Duties that encompass the approval or the process of cases of presumed disloyalty, subversive activities or disaffected personnel.

e. Any other activity or position designated as sensitive post by the senior command chiefs.

3. Usually, we refer to those functions that require access to CONFIDENTIAL information or to higher security classification. In order to occupy a sensitive position it is not necessary for the individual to be involved in the creation of classified information , nor to act in making decisions related to it. For example, the typist that copies classified documents has access to the information and therefore, occupies a sensitive position. The keeper of files does not have to read the classified documents that he handles has access to classified information and also occupies a sensitive position. All positions of officers, NCO's, and enlisted men are considered sensitive by virtue of their rank.

a. Up to this point, the sensitive positions that have been mentioned have something to do with classified information. However, it is possible to occupy a sensitive position or perform in a sensitive post without having anything to do with classified information. These functions or duties concern the teaching programs, briefing of personnel of the armed forces, including the training for such duties.

b. In this case, the sensitivity of the position is not determined on the basis of access to classified information, but on the basis of the influence that the personnel of instruction programs may have on the military personnel and their ways of thinking. The sensitive classification is reserved to persons of the military personnel that produce or administer the program. The recipients, the military personnel receiving training are not considered participants of a sensitive function or position.

c. Finally, the sensitive positions involve the process of investigation of allegations of disloyalty, subversion, and disaffection. Because of our duties and responsibilities, we, the intelligence personnel, are included in the category of sensitive positions.

d. These are the sensitive functions that required a Security Certificate. The commander decides whom to authorize such certificate based on the information that we, as Agents, provide through our investigations of personnel security.

4. WHY ARE INVESTIGATIONS OF PERSONNEL SECURITY NECESSARY?

ARE ALL MILITARY PERSONNEL CONSIDERED DISLOYAL?

a. Senior chiefs of Military Intelligence have given some reasons for carrying out investigations of personnel security. Among them:

(1) Any intelligence agency that does not believe it could be penetrated any day, by any of its officials, from the concierge to the director, would be very complaisant and we would be criminally negligent if we do not function under such supposition.

(2) We have to act under the supposition that our adversaries are as cunning as we are and that they will be able to enter every now and then.

(3) The security of the nation demands constant vigilance in order to maintain our adversaries outside, and prevent them from obtaining information and to uncover and remove them as soon as possible.

4.[sic] How can we keep our adversaries from entering?

(1) The proper authority will be the one who determines the need for a personnel investigation of an individual. This authority usually is the commander.

(2) The request is sent to the Intelligence Officer of the Staff at national level, who in turn orders his control office to initiate an investigation and refer it to the CI unit for investigative action.

5. An investigation of personnel security is used to find out the following:

1. Loyalty
2. Discretion
3. Character
4. Integrity
5. Morale

of an individual that will give information upon which a decision would be made on whether the individual will be posted to a specific position that requires access to classified material which is consistent with the interest of national security.

6. The action agency will be the same commander who made the request. The commander must take a decision in each investigation. The decision will be based on the information contained in the investigative reports provided by Counterintelligence.

7. The fact that the person enters voluntarily into one of the armed forces is no proof of loyalty, because:

a. The individual could be intending to accomplish an illegal/nefarious act.

b. Could be intending to gain access to classified military information.

c. Could be intending to deliver such information to an enemy agent, present or potential, to obtain military experience in order to be able to apply it against us when the occasion arises.

7.[sic] Acts like swearing allegiance (in writing), going to church, etc. are only manifestations of loyalty and respect that could be used to over up ulterior motives. These manifestations cannot be accepted as proof of loyalty, although they have much value as indicators of the right direction.

D. INVESTIGATIVE REQUIREMENTS:

1. (How does an investigation start? EXAMPLE:

a. Suppose a new typist will have to work with classified information, and therefore, needs access to same. Since he never had previous security authorization to work with classified material, the commander, responsible for the security of his command, requests a security investigation of personnel for the new typist. The request goes up to national level to the Staff Intelligence Officer whose function is to provide information on security. On the other hand, the counterintelligence of the unit directs the investigation of personnel security of the new typist.

b. In order to establish the loyalty of a person, the lack of disloyalty has to be proven. In order to prove it, the qualities and weaknesses that might lead a person to commit a disloyal act are searched.

c. Among the things looked for to prove disloyalty are:
1) Vengeance
2) Desire for material gains
3) Desire for more prestige
4) Friendship
5) Ideological tendencies

d. Among the weaknesses that make a person susceptible to committing a disloyal act under pressure are:

1) Close relatives in foreign countries.

2) Big financial investments in foreign countries.

3) Jealousy

4) Credibility

5) Weak character

6) Serious guilty episodes in the past

7) Debts

8) Use of Narcotics

e. Absence of the factors indicated above is an indication of loyalty and confidence on the individual under investigation. Only a small percentage of the investigations of personnel security show that an individual is disloyal. Our work as CI Agents is to find that small percentage of disloyal persons, and prevent them from getting access to the type of information that could be damaging to the national security. We discover the weak points within the national security, it is up to the commander and the agency to act, eliminating them from sensitive positions.

f. Description of each one of the factors mentioned above, which could affect the loyalty of a person:

1) VENGEANCE: Could be one of the strongest motives. Hate corrupts the moral value in such a way that the person could do the utmost to betray his country in order to take revenge against a person or group he hates.

2) MATERIAL GAIN: Some people yearn so much for personal gains that do not stop at anything to attain their goals. We do not condemn ambition and the innate desire to advance in life, but we do condemn the persons that want to amass riches without taking into consideration the ethics of society.

3) PERSONAL PRESTIGE: This motivation applies to those persons whose main ambition is for power, power above all, to demonstrate the work their superiority as leaders.

4) FRIENDSHIP: Some persons of high integrity commit acts against national security because of friendship ties to another persons.

5) IDEOLOGICAL BELIEFS: A person that has hostile beliefs against its own country is very vulnerable to be approached by agents or subversive groups.

6) CLOSE RELATIVES IN FOREIGN LANDS: For a long time, threats of mistreatment against loved relatives who are under the regime of a threatening power have been used. The Soviets have widely applied similar techniques, currently, as a means to obtain support and cooperation.

7) INVESTMENTS IN FOREIGN COUNTRIES: Due to human nature, there are many persons who consider that material riches are more important than the integrity of moral principles. When these persons are in danger of losing their investments in foreign countries, they can be persuaded to betray their own country.

8) JEALOUSY: One of the strongest motivations used by cunning agents in order to induce loyal persons to commit hostile acts against their own country.

9) CREDIBILITY: In this category are classified those persons that believe in everything literally and do not find anything wrong in other persons. This type of person is almost always an idealist and sometimes could be used as an instrument by unscrupulous agents. Credulous persons by stupidity are not used frequently because of the poor quality of information that they might obtain, although in some occasions they could be used as "bait" for sabotage acts, strikes, and public disorder.

10) A person with a weak character can be easily dominated by another one and is an easy prey for subversive elements looking for a servile assistant.

11) DEBTS: The persons that have gotten into substantial debts always try ways to recover their losses quickly and easily. These persons constitute a definite security risk, and is very vulnerable because he can be persuaded by a considerable sum of money. We all know the saying: "EVERY ONE HAS A PRICE," therefore, the price of all persons in this category is relatively low.

12) USE OF NARCOTICS: This category does not need explanation. We all know that the drug addicted commit crimes in order to maintain their habit.

13) GUILTY COMPLEX: As human beings, many of us have experienced certain episodes in the past for which we may feel ashamed. The enemy agents that have the mission to recruit agents/sources, do not hesitate in taking advantage of such experiences to force the cooperation of the individuals for subversive conspiracy. The threats to divulge such episodes has always been a powerful wedge to force a person to commit illegal acts.

g. These are some of the factors that we must look for during an investigation of a person to be employed in a confidence position. When we discover indications in any of them, the investigation is broadened in order to:

1) approve them
2) reject them. really bad translation

h. Looking for the bad side of a person might seems like a cynical act, but we are in a cynical occupation that has demonstrate throughout the years and by experience, that this is the only way to approach an investigation.

i. The experienced investigator does not accept from the start any information that has not been checked.

j. A very important part in the life of a CI agent is his behavior during an investigation of personnel security. The behavior of the agent ensures whether he will obtain the information or not. The interview is a very emotional situation for many persons. Even though you identify yourself as am agent of Military Intelligence, they will take it as though you are an agent of criminal investigations (police). It depends on you and your behavior during the interview whether it will have positive results or not.

5. CERTIFICATE OF SECURITY AUTHORIZATION

a. After the action agency (the commander) finishes with the study of the personnel security investigation results, he proceeds to carry out one of several lines of action:

1) He might ISSUE a certificate of security authorization
2) He might DENY the certificate of security authorization
3) He might REVALIDATE a certificate previously <u>invalid.</u>
4) He might INVALIDATE a security authorization previously issued.

6. TYPES OF INVESTIGATIONS OF PERSONNEL SECURITY

a. Usually we are interested on two types of investigations of personnel security:

1) To check National Agencies (CNA)
2) Investigation of Personal History (IPH)

b. The type of investigation required at any time depends on the category of the classification of the defense information to which access is required, and the citizenship of the individual concerned.

c. CHECKING THE FILES OF NATIONAL AGENCIES

1) It consists on an examination of the files of those national agencies that might have information related to the loyalty and reliability of the individual. The Control Office determines which agencies shall be checked in all the cases:

a) The Internal Security Agency (DNI)

b) Index of Investigations of the Armed Forces

2) Internal Security Agency: The files of crimes and subversive activities will be checked during all the investigations. It should include fingerprints of each applicant.

3) National Level of the Army:

a) Staff Intelligence Office

b) Director of Personnel Administration (military)

c) Chief of the Military Police

d) Index of Central Archives (Minister of Defense)

These are checked when there are indicators that the individual is or have been employed by, or is owner of, a company that has had classified contracts with the Minister of Defense.

4) National Level of the Navy

5) National Level of the Air Force

6) Archives of the Government Ministries

7) Other Investigative Agencies.

7. CHECKING NATIONAL AGENCIES (CAN) AND INQUIRIES IN WRITING:

a. We have already discussed CAN. Parts of the investigations of files include the Inquiries in Writing. This is done for the following agencies and individuals:

1) Local Agencies of Law Enforcement

2) Previous supervisors of the individual

3) References given by the individual

4) Learning schools and institutions

b. The Written Inquiry is usually a mimeographed letter distributed to the character references and credit references given by the individual, requesting from them a written report on everything that they know about the individual.

8. INVESTIGATION OF PERSONAL BACKGROUND:

The second type of investigation of personnel security is the investigation of personal background. This category constitutes the majority of the investigations that you will perform as CI Agents.

a. Components of an investigation of Personal History (Background):

1) Checking with National Agencies (CAN)
2) Birth certificate
3) Education

4) Employment
5) References
6) Investigations in the neighborhood
7) Criminal background
8) Military service
9) Connections abroad
10) Citizenship
11) Credit Record
12) Organizations
13) Divorce record

b. Checking National Agencies (CAN) is to verify the files of national agencies with regard to the loyalty, morality, discretion, character and integrity of the individual.

c. Birth Record: Usually we do not check birth records, unless there is discrepancy in the birth dates of other recorded files.

d. Education: The files of all the schools and learning institutions attended by the individual. Interviews can also be had with teachers and professors of the individual in order to get more personal and intimate information of the individual.

e. Employment (occupation): We are interested in the degree of efficiency at his work and the reason why he terminated his employment.

f. References: In the majority of the cases we must assume that the personal references given by the individual will be partially or totally in his favor. There are three reasons why we verify the references:

1) It is possible that the person indicated in the Personal History as a friend, might not be so friendly with the individual.

2) A friend might reveal damaging information without being conscious of it.

3) The references are a good source to obtain "developed sources." These are persons that have knowledge of the background of the individual but have not been given as references in his application.

g. Investigations in the neighborhood: Valuable information is obtained of the personal life of the individual. Mainly what is done is a compilation of gossip (rumors). But if this gossip come up again in other agencies, they could be taken as valid.

h. Record of criminal background: It could be requested by mail or through Liaison investigations. The information obtained from these records must be verified with the court register and judicial procedures.

i. Military Service: The type of leave or discharge is checked in order to verify if it was because of disloyalty, subversion, indiscretion, or moral perversion.

j. Connections abroad:

1) Determine up to what point the individual has investments in foreign countries. What is the amount of money invested by the individual in these countries.

2) Another point that should be examined is whether the individual has relatives in those countries. It is possible that the foreign country may put pressure against the individual by using his relatives as an excuse.

k. Citizenship. The citizenship of an individual and his parents could be verified through the records of the Immigration Service.

l. Travel abroad:
1) Dates of departure
2) Destination
3) Purpose of Travel. Activities that the individual was involved in during his stay in that country. It is possible for the individual to have been involved in some difficulties in that country.

m. Credit Record: Credit agencies are contacted, credit loaners, where the individual has resided for considerable periods of time. Through these records the integrity of the individual can be determined.

n. Organizations: Investigate whether the individual was a member or was affiliated or sympathizer, with any organization, association, movement, group or combination of foreigners or locals that have adopted or manifested a policy of defending or approving enactment of actions by force or violence in order to deprive other persons of their rights as dictated by the country's constitution.

o. Divorce records: It is used to prove or contradict the information already included in his Personal Background (history).

9. EVALUATION OF THE INFORMATION OBTAINED:

a. It is the duty of the investigator to point out if the information obtained during the investigation are "Facts", "Opinions." or "Rumors." There are three ways to comply with this requirement:

1) Description in Words: Indicate by means of a description in words the degree of Reliability of the confidential informants, when submitting the information received from them. The description in words is used only to describe the information obtained from reliable sources. EXAMPLES:

a) The Source (So and so), who has submitted confidential information in the past informed the following:

b) The Source (So and so), reliability unknown, who knew the Subject for the past ten years, informed the following:

2) Notes or Remarks by the Investigator (Agent): are remarks by the agent which can be included in the report to add validity to the information provided by the source, or else to detract validity to such information. EXAMPLE:

a) " The source was very nervous during the interview."

b) "His statements (the Source's) regarding dates and places were very generalized and sometimes gave the impression of not being sure of himself."

3) Appropriate phrases: Using certain appropriate phrases in the report will help the control agency to determine more accurately the validity of the information provided. EXAMPLES:

a) "The Source said that ...."

b) "The Source provided the following rumor..."

10. ENDING THE INVESTIGATION:

a. The action agency bases its determination regarding issuance of authorization certificates to classified material on the investigation carried out by the CI Special Agents:

b. The investigation that you have carried out will determine the future of the individual, and therefore each investigation must be as complete as possible.

c. In an effort to provide a superior investigation, the Agent should:

1) Obtain all possible information.

2) Support all the conclusions with facts.

3) Identify all the opinions as such in the investigation report (Agent's Report)

4) Explain all the leads that were not followed.

5) Obtain enough information during the course of the investigation in order to enable the Action Agency to adopt a final action upon receiving the results of the investigation.

11. AGENT'S ATTITUDE

In order to combine all the desirable requirements of a CI Special Agent, while performing his functions in the field of intelligence, you should always have:

a. Know the significance of the words loyalty, discretion and reputation in order to be able to gather the required information for the Action agency.

b. Keep in mind the purpose of the investigation so that the findings will reflect the information required by the Action agency.

c. Be impartial, absolutely, in order to do justice to all; to the SUBJECT of the investigation and to the national government.

d. Be diplomatic while performing your duties as investigator, in order to obtain the information desired without wasting any time.

e. Maintain a professional stance at all times because it will reflect your quality as an agent, the quality of the CI service and of the Army.

f. Avoid accusing the interviewee because you need to obtain certain information from that person, and if he becomes scared, he will not be able to talk.

CHAPTER VIII

INTERROGATION PHASE/TECHNIQUES

INTRODUCTION:

The interrogation phase/techniques for questioning have a very unique value because they will cover all the interrogatives. The ability to ask questions is as important as the investigation that is being carried out. Without a good knowledge of how to address his questions, many times valuable intelligence information could be lost or answers are given that are contrary to what the source provided.

GENERAL:

a. Usually, the interrogation phase/questioning techniques starts when the source starts answering questions pertinent to the specific objectives of the interrogation/interview.

b. The questions must be sufficiently comprehensive to ensure that the subject of interest has been completely exploited.

c. All the answers obtained from the Source must established the basic interrogatives which are:

(1) Who
(2) What
(3) When
(4) Where
(5) Why
(6) How

d. All your questions must be presented in a logical sequence in order to be sure that the significant topics or objectives have not been neglected.

e. Frequently a series of questions are used, following a chronological sequence of events, but it is by no means the only logical method of making an interrogation.

[one page missing from the original]

(3) Non Pertinent Questions:

(a) Non pertinent questions are those that have nothing to do the with objectives of the interrogation/interview. When pertinent que non-pertinent questions are carefully mixed, the Special Agent [SA] could hide the real purpose of the investigation and make the Source believe that a relatively insignificant matter is the basis for the interrogation/interview by asking pertinent questions in a casual manner. For example:

* Emphasizing questions and details that are not important.

* Dwelling on non-pertinent topics that the Source seems unwilling to discuss.

(b) One of the techniques for which non-pertinent questions are used is to make the source relax, and then go back to pertinent questions in order to obtain the information desired.

(c) Another use for non-pertinent questions is to break the "train of thought" of the source. This is particularly important if there is suspicion that the source is lying.

Always have in mind that the Train of Though is an effort by the Source to concentrate possibly to come up with a lie. The SA could break the concentration by introducing suddenly a completely unrelated question, and afterwards returning to the pertinent topic.

(4) Repeated Questions:

(a) The repeated questions are used as a means to ensure precision, particularly when the SA suspects that the Source is lying.

(b) One of the techniques is to repeat the same question in another way or disguised.

(c) The repeated questions also are useful to ensure precision in the details, such as places, names, dates, team components and similar topics.

(5) Direct or tricky questions:

(a) The way you express the questions have a direct relationship with the response of the Source. A question can be made in different ways. Example:

"Where did you go last night?"
"Did you go last night to general headquarters?"
"You did go to general headquarters last night?"
"Didn't you go to general headquarters last night?"

(b) The first example (where did you go last night?) is a direct and simple question that requires a narrative answer. This type of question usually produces the maximum amount of information and provides a great number of leads that can be followed or exploited by the SA.

(c) The other three examples are tricky questions in that they are suggesting the answer.

(d) Tricky questions tend to suggest the source the response that he thinks the SA wants to know, and also limits the number of details given in the answer.

(e) As a general rule, the tricky questions are not good for the purpose of interrogation/interview, but could be used efficiently as a means of verification, means of strategy, or as a means of pointing out with precision at specific details.

(6) Combined Questions:

(a) Combined questions are those that contain more than one question. This type of questions should be avoided because they could be evaded easily and sometimes are difficult to understand. For example:

"What kind of training did you receive at the basic training center of the enemy forces, and what kind of training did you receive afterwards at the advanced training center of the enemy forces?"

(b) As you have noted in the above example, the source may answer only one, both or none of the questions, and the answer given may be ambiguous, incomplete or both.

(7) Negative Questions:

(a) Negative questions are those that confuse and give deceiving or false answers. This type of question could suggest two answers. For example:

"Don't you know whether Colón went to General Headquarters last night?

(b) If the SA is not aware of the negative question, with all probability he will extract an answer that the source never wanted to give.

(8) Precise and Brief Questions:

(a) All questions should be precise, brief and to the point. There should be no doubt in the mind of the source of what the SA wants to know. This type of question is identical to the direct question and limit the level of the Train of Thought of the Source since it should require a narrative response.

(9) Questions Expressed Simply:

(a) The SA must use simple questions. Avoid convoluted words (words whose meaning other persons might not know).

(10) Reinforcement Questions:

(a) The reinforcement questions are those used to impart emphasis at a certain point of the interrogation/interview. During the interrogation/interview the SA must remain alert to detect and exploit the statements by the Source that indicate that he has valuable intelligence information, besides the one which is pursued in the present interrogation/interview.

3. Information from Rumors:

(1) Rumors can provide valuable information. However, rumor must be classified as rumors.

4. Conclusions:

(1) The last step of the interrogation/interview is to obtain any additional conclusions, statements, remarks or evaluations of a specially qualified source.

(2) When the SA receives such information, he must also obtain the facts on which the source based his conclusions and/or evaluations.

5. Interrogation/questioning techniques Phase

a. The interrogation/questioning techniques phase is what "truly makes a Special Agent" since it would be worthless to have an excellent "planning and preparation" and a wonderful "approach plan" if the "Interrogation/Questioning Techniques Phase" is not exploited to the maximum advantage in order to obtain the greatest intelligence information possible.

b. Types of Interrogations/Interviews:

The SA usually follows two general rules (the direct or indirect interrogatory/interview). The essential difference between the two lies on whether the source knows or does not know that he is being interrogated/interviewed.

c. The Direct Interrogation/Interview:

When we use the direct interrogation/interview, the source is conscious of being interrogated/interviewed, but knows or does not know the real objective of the interrogation/interview.

d. Advantages of the Direct Method:

(1) Consumes less time.

(2) Easier to carry out (nothing to hide)

(3) Allows the SA to make continuous verifications of the information that he is receiving from the source.

e. Disadvantages

(1) The source does not want to be a stool pigeon.

(2) He is afraid for his life (or his comrades')

(3) Thinks that he can obtain something in exchange for the information offered (his own benefit).

f. Indirect Interrogatory/Interview:

This form of interrogation/interview is characterized by getting information through deceit and trickery without the source knowing that he is being interrogated.

g. Advantages:

(1) The information extracted is almost always true (no reason to lie.)

(2) It is useful for extracting information (even) from the most difficult sources.

(3) It serves for exploiting a big human weakness (the desire to talk).

h. Disadvantages

(1) A great deal of skill is needed.

(2) It consumes too much time and personnel.

(3) We do not know really whether the source really wants to cooperate/confess everything.

5. Use of techniques:

a. Have in mind that both types of interrogation/interview can be used at the tactical as well as strategic level.

b. Determining factors for the direct interrogation/interview:

(1) Very limited time (TACTICAL LEVEL)

(2) To use for immediate operation

(3) SA does not have much training

c. Determininq factors for indirect interroqation/interview:

(1) Said operation/mission does not have immediate tactical importance.

(2) The goal to be attained is at strategic level.

Example: To know the enemy capabilities to sustain hostilities for long periods of time.

6. Selection of the Source:

a) The criteria for the selection of personnel to be interrogated/interviewed could vary for innumerable reasons:

1) Time limitations
2) SA availability
3) Skills of the Ae (who in general serve as selecting officers).

4) Quality and quantity of information that the sources could have.

CHAPTER IX

~~INVESTIGATION OF~~ PERSONNEL SECURITY INTERVIEWS

INTRODUCTION:

The interviews of personnel security [illegible] enable~~s~~ us to obtain truthful information to help us in our determination to offer a person access to classified information that might affect national security. These interviews are done normally with a person that has known the SUBJECT being investigated.

GENERAL:

1. Before beginning the interview we have to do good planning and preparation for the interview. The following steps must be taken if at all possible:

a. Identify the individual that will be interviewed.

NOTE: FOR THIS KIND OF INTERVIEW, A PRELIMINARY DATA SHEET WILL GIVE US THE CHARACTER THAT WILL BE GIVEN TO THE INTERVIEW.

b. Prepare the questions that will be made.

1) Develop questions que will extract information regarding the following matters related to the SUBJECT:

a) His loyalty
b) His character
c) His reliability
d) If he is or is not adequate to fill a position of confidence.

c. Prepare questions that will allow the source to answer in an open and spontaneous manner (narrative form).

d. Avoid questions that only require "YES" or "NO" as an answer. Examples: Is your name Miguel?

e. Prepare your questions using the basic interrogations (always have in mind the basic interrogations during the interview):

1) How
2) When
3) Who
4) What
5) Where
6) Why

f. Obtain the required forms, such as Sworn Statement, signed.

2. Once planning and preparation have been completed CONTACT THE INDIVIDUAL TO BE INTERVIEWED.

a. Try to make contact and carry out the interview during working hours at the individuals work place (or where appropriate depending on the situation, if necessary make an appointment with the Source).

3. Once the meeting has been arranged and you meet the Source, carry out the interview.

a. Identify yourself and show your official credential (always remember that you are the representative of a national government and that you are a Special Agent).

b. Ensure/certify that the Source himself knows the SUBJECT (if necessary ask him for an identification card).

c. Inform the Source of the purpose of the interview (Example: the purpose of this meeting is to obtain information on .... who is considered for a confidence and responsibility position with the national government ....)

d. Obtain positive identification from the Source.

e. Try to gain and keep the confidence of the Source in such a way that he will feel at ease with you.

f. Make the arrangements for the interview to take place in a quiet place and free of distractions.

NOTE: IF YOU HAVE A RECORDER AVAILABLE AND THE SOURCE DOES NOT OBJECT, EXPLAIN TO ;HIM THAT YOU WANT TO USE TO PREPARE YOUR REPORT OF THE INTERVIEW IN THE MOST ADEQUATE WAY.

g. Obtain and make notes of the information of the identification of the Source, including:

1) Name and rank
2) Position
3) The complete designation of the unit and its location or place of work and position.

h. Inform the source that the interview is considered official business and warn him that he cannot discuss its content with strange persons to Military Intelligence.

i. Ask questions to obtain information from the Source regarding:

1) Day, time, place and circumstances when he met the SUBJECT.

2) Day, time, place and circumstances when he last saw or communicated with the SUBJECT:

3) Frequency of contact between him and the SUBJECT:
1) professional contact
2) social contact

4) Any length of time over 30 days when he did not have contact with the SUBJECT:

5) Number of times and frequency of contact since he saw the SUBJECT last and method of communication.

j. Ask the Source questions to determine his knowledge of the following regarding the SUBJECT:

1) Date of birth
2) Place of birth
3) Use of nicknames
4) Military units to which he belonged (if applicable).
5) Residences
6) Education (where did he study and to what level).
7) Civilian employment
8) Family
9) Hobbies/interests
10) Partners/business associates

k. Questions asked to obtain the Source's opinion regarding:

1) The honesty of the SUBJECT
2) The confidence on the SUBJECT.
3) Can de SUBJECT be depended on?
4) Maturity of the SUBJECT
5) Morality of the SUBJECT
6) Mental and emotional stability of the SUBJECT.

l. as the Source if he has knowledge of any problem that the SUBJECT might have had with police authorities.

m. Ask the Source if he has knowledge of:
1) whether the SUBJECT uses or has used illegal drugs
2) whether the SUBJECT abuses prescription drugs
3) whether the SUBJECT has the habit of gambling.
4) The financial stability of the SUBJECT.
5) Use or abuse of alcoholic beverages
6) If he is member, goes to meetings or support any organization that intents to overthrow the national government.

7) If he is a member, or support any organization that tries to deny civil rights to a person or group of persons.

8) What is the professional reputation of the SUBJECT.

9) Whether the SUBJECT has made previous trips or long trips abroad.

10) Social reputation

11) Relatives living abroad

12) Business contacts in foreign countries.

n. Ask the Source if the SUBJECT is loyal to the government.

o. As the Source if he would recommend the SUBJECT for any position of confidence and responsibility with the national government.

p. THE SOURCE SHOULD BE ASKED TO PREPARE A SIGNED, SWORN STATEMENT; .sworn statements are required when:

1) The source does not recommend the SUBJECT for a confidence position.

2) The source gives negative or derogatory information on the SUBJECT.

3) The information given by the Source does not conform with the negative information previously received.

q. Obtain leads (additional contacts). Determine whether the Source knows other persons that know the SUBJECT and his activities.

r. Determine whether the Source wishes his name to arise as provider of this information in case the SUBJECT requests it.

s. End the interview.

1) The Source has to be reminded that none of the contents of the Interview should be commented with anybody else.

2) Thank the Source for his cooperation and bid good-by.

4. Prepare the required reports.

CHAPTER X

HOW TO OBTAIN A SWORN DECLARATION

INTRODUCTION:

During its functions as a Counter Intelligence Special Agent you must get a sworn declaration from the persons whom you have interviewed. These sworn declarations will help you determine the truth of the persons interviewed as well as recognizing if the information that they have given has any connection with your investigations.

DEVELOPMENT:

A. Definition of a Sworn Declaration:

A Sworn Declaration is a written statement about facts, given voluntarily by a competent person who is a witness, who states under oath that the content of the statement is true.

B. The Sworn Declarations must be obtained from the following categories of interviews:

1. Witnesses with direct or personal knowledge of the incident.

2. Sources who provide credible unfavorable information. Credible unfavorable information is defined as: Information related to loyalty and attitude of a person, who appears to be honest, and so who could make a probable base to take adverse action.

e. The sources who refuse credible unfavorable information. Information that has been refused its defined as: That information that was refused (without validity).

4. SUBJECTS of an interview.

5. Suspicious persons who are citizens of the country.

6. Persons who have been accused and that are not citizens of the country.

C. You may obtain this information during the interviews using the interrogation basic techniques in an efficient way.

5. The next four blocks will note the complete information about a person who is making a sworn declaration. The following information is included in block E.

a. Complete name of the person

b. Personal identity number

c. Grade or civil rank

d. Military unit or civil residence

F. You must aid the interviewee to write a declaration using one of the following methods:

1. Narrative method

a. The narrative method allows the interviewee making a declaration to write the information in his own words. This method is normally used when preparing the declarations of Sources, Witnesses, or Unscheduled persons.

b. The Sworn Declarations made by a source must have a summary declaration explaining the social degree or professional association between the source and the subject. This must have the facts and circumstances of the facts that support or contradict the unfavorable credible information and answer all the basic interrogations.

2. Question and Answer Method

a. When you are preparing a sworn declaration for a subject, accused or suspicious person use the question and answer method so as to ensure the verbal file in the interview. The question and answer method has both questions that you make and answers from the interviewee. This method allows you to limit to just the information contained in the declaration that is pertinent.

b. The sworn declarations made by a subject, source or accused persons must contain, in addition to the facts and circumstance the following information:

1. An explanation of the purpose of the interview.

2. A declaration of recognition of the provisions of privacy according with the national government and these provisions must be explained.

3. A declaration of recognition that the SUBJECT was advised of his constitutional rights and that he denied these rights in writing noted in the certified text of the SWORN DECLARATION/LEGAL RIGHTS/USE OF A LAWYER.

4. A petition to have an interview under oath and the answer.

5. A complete personal identification of the interviewee.

6. A final question to find out if the interviewee wishes to add or change the declaration.

3. A combination of the two methods mentioned above normally provides the best result. The person interviewed is allowed to express himself and afterwards you may use the method of questions and answers to obtain specific information that has been omitted previously. This method also allows you to clarify the areas where the interviewee has not been clear in the declaration.

G. All sworn declarations will be written in first person. The vocabulary and the grammar of the interviewee must be used during the entire process, including vulgarities if they are pertinent or provided as part of the actual interviewee's appointment. Expressions written in parenthesis, abbreviations, facts in military style and investigative jargon or the use of capital letters only used by the counter intelligence agents must not be used.

H. Use additional pages to complete the body of the declaration. The additional pages are used when the sworn declaration does not fit in the second page of the document.

I. When typing the sworn declaration, write the declaration as close as possible to the margins of the document, or write a line towards the margin when the declaration or sentence does not reach the margin.

J. At the end of the sentence of the sworn declaration, include the phrase, "Declaration Finished".

K. In a sworn declaration that has been typewritten, have the interviewee put his initials at the beginning of the first sentence and in the last sentence of each page, as well as putting his initials on the side of any correction or errors. The sworn declarations made in handwriting do not need the initials unless there are corrections. Corrections made to the sworn declarations must be done in ink and ball point pen preferably in black ink, but keep in mind that the interviewee must put his initials next to the corrections.

L. Complete the section under the page including the number of the page and the total of pages (page from page) and then you must make the person making the declaration put his initials in the upper part of each page in block F.

M. Complete the section of the declaration writing down the name of the interviewee in blank sections in block H.

N. Make the interviewee read the sworn declaration and make sure that he understands it.

O. Make the interviewee repeat the oral oath. If the interviewee does not wish to take the oath, you must not try
to persuade him to change his mind. But, you must explain that a declaration that is not under oath could be used as evidence as well as you must explain that the meaning of the oath, and the penalties for submitting a false declaration.

P. Make the interviewee to sign the sworn declaration. If the interviewee took the oral oath but does not wish to sign the sworn declaration, do not try to change his mind. Explain to him that the oral oath and not his signature is what makes this document a sworn declaration and that such document will be sent to the appropriate destination. Allow him the opportunity of making any changes to his first declaration. But, never destroy the original declaration.

Q. Write down the place and the date where the oral oath was obtained in block J.

R. Sign the document in block K, and typewrite the complete name of the counter intelligence agent in block L.

S. Write down the authority that the counter intelligence agent has in block M.

T. Make the witness (if it applies) sign the sworn declaration. The witness signs the sworn declaration affirming that the interviewee understands the content of the sworn declaration and that the interviewee signed such declaration in your presence. THE WITNESS DOES NOT HAVE TO BE PRESENT DURING THE INTERVIEW, ONLY ONE WITNESS IS REQUIRED DURING A SWORN DECLARATION, UNLESS THE INTERVIEWEE WISHES A WITNESS TO BE PRESENT DURING THE INTERVIEW.

U. If the interviewee wishes a copy of the sworn declaration provide him with a copy under the conditions that the sworn declaration is not classified.

NOTE: If the sworn declaration is classified make sure that it is classified according to the SOP.

V. Complete the appropriate reports, write down and add all the details.

NOTE: When a sworn declaration is taken from a person that does not speak the national language, copies of the declaration must be prepared in the language spoken by the person. If necessary, use an interpreter for this purpose. Both declarations must have a statement indicating that the content of the declaration is complete and without errors. The person who transfers the document must sign the declaration and indicate that he is competent. The counter intelligence agent must supply the oath to the interpreter before the interpreter signs the declaration.

CHAPTER XI

UNSCHEDULED INTERVIEWS

INTRODUCTION:

Frequently you will find an interview in which the person comes to the counter intelligence office to give information. This interview is not prepared beforehand, but it must be professional at the moment it takes place.

GENERAL FACTS:

1. Once the person comes into the office you must:

a. Be courteous and professional.

b. Show your official badge (credentials).

c. Obtain any personal identification.

NOTE: GAIN THE PERSON'S CONFIDENCE AND BE NICE AND ALERT. THE EFFORT TO WIN THE PERSON'S CONFIDENCE MUST COME FROM THE MOMENT THE PERSON ENTERS AND CONTINUE THROUGH THE INTERVIEW.

d. Determine the purpose of the source's visit.

1. <u>Definition of an unscheduled interview</u>

An unscheduled interview is that in which the person comes voluntarily to the Counter Intelligence office and offers information that he thinks has value to the military intelligence. Frequently the person has some personal interest (money) in giving this information to the Counter Intelligence.

2. Some persons that fall within this category (unscheduled interviews) are:

a. Native persons (residents of the same area where the incident occurred).

b. Deserters

c. Refugees or displaced persons

d. Tourists and other persons visiting the area.

e. Participants in international conferences.

f. Enemy agents under low rank, or importance.

g. Persons who are only a nuisance to military intelligence. That is those who give constant information that is useless to the CI.

2. Once the person has come to your office start a Review of Files (the review is done normally when a person is busy and this review is done normally by his assistant):

a. Determine if the name of the person appears in the list of persons that are only nuisances to the CI.

b. Determine if the National Police, Military or Treasury has a file about this person.

3. If the review of the files indicate that the person is a nuisance to military intelligence:

a. Thank the person for his information.

b. Close the interview and walk out the person, be polite when doing it.

4. If the review of files does not indicate anything negative regarding the person, continue with the interview.

5. Once the assistant gives you the results of the review of files you may carry on with the interview:

a. Ask the person permission to use a tape recorder during the interview. Explain to the person that this will help you prepare the report for this interview, and obtain all the information that he brings without making mistakes.

b. Turn on the tape recorder only if the person allows you to.

c. Take the oath of truth from the person (Example: You pledge or swear to tell the truth, the whole truth and nothing but the truth). The oath of truth must be taken standing up (if applicable) and with the right hand raised (if applicable).

d. Ask the person to tell you the whole incident, or whatever information he has.

1. Encourage the person to give you information in his own words.

2. Listen carefully and take mental notes of the areas of interest from the information given by the person.

3. Don't take written notes while the person is telling you the incident.

4. Don't interrupt the person.

NOTE: IF THE PERSON GOES OFF THE SUBJECT, TACTFULLY LEAD HIM TO THE MAIN THEME.

e. Go over the story the person has given you:

1. Assure the person that the information he brought will be kept in strict confidentiality.

2. Go over the story the person has given you covering all the points of emphasis and to clarify all discrepancies or contradictions.

3. Write down all leads that come up.

f. Obtain information from person's history to help in the evaluation of the information. This information of history must include:

1. Identity (complete name, rank, and personal identity number.)

2. Date and place of birth

3. Citizenship

4. Present and past addresses

5. Occupation

6. What motivation he had to come to report the information

g. Develop the secondary information: Frequently the story and history of the Source indicate that it is possible that he would have additional information of interest to military intelligence.

NOTE: IF DURING THE INTERVIEW, THE SOURCE OF INFORMATION IS NOT WITHIN JURISDICTION OF THE MILITARY INTELLIGENCE, PUT THE SOURCE IN CONTACT WITH THE AGENCIES OF GOVERNMENT THAT COULD BE INTERESTED IN SUCH INFORMATION. IF THE SOURCE DOES NOT WISH TO TALK TO ANYONE ELSE, MAKE NOTE OF THE INFORMATION AND PASS IT ON TO THE INTERESTED AGENCY.

h. Obtain a sworn declaration, signed by the source.

i. Explain to the person the official nature of the interview and caution him not to talk with anyone about what happened during the interview.

6. Close the interview:

a. Advise the Source that it is possible that he may me interviewed again. Determine if he is willing to participate in another interview.

b. Make arrangements for the new contact.

c. Close the interview in a nice manner.

d. Walk with the Source to exit the office.

7. Prepare the reports/necessary reports.

CHAPTER XII

WITNESS INTERVIEW

INTRODUCTION:

Interviewing the witnesses of an incident offers the CI agent the opportunity of verifying information that is provided by another source. It helps us clarify doubts that we may have about the truth of the information collected.

GENERAL FACTS:

1. DETERMINE THE NEED TO HAVE A WITNESS INTERVIEW:

a. You must answer the incidents/activities and interview all the existing witnesses, who were in the area where the incident occurred.

b. You must answer the tasks that are presented by the preliminary sheet.

2. You must determine if the witness had personal knowledge of the incident.

3. Plan to carry out the interview in a quiet place, free of interruptions.

4. Identify yourself to the witness and show the Official badge.

5. Identify the witness examining his badge and any other identity card that he may have.

6. Try to win his trust and make him feel secure.

7. ASK PERMISSION FROM THE WITNESS TO USE A TAPE RECORDER DURING THE INTERVIEW. EXPLAIN THAT THE TAPE RECORDER WILL HELP YOU TO COMPLETE THE REPORTS MORE ADEQUATELY.

8. Turn on the tape recorder if the witness allows you.

9. Ask the witness to tell you his story.

a. Take general (mental) notes about the information brought by the witness.

b. Take detailed notes of the unclear or doubtful areas to develop them later in more fully.

10. GO OVER THE STORY WITH THE WITNESS:

a. Discuss the story with the source in detail, covering all outstanding points.

b. Ask questions in detail (use the basic interrogations) about specific areas that you noted while the witness told the story.

c. Clarify any doubtful area .

d. Take detailed notes.

e. Use drawings, sketches, charts as supplements if these may help to clarify any information, or to interpret the incident as it happened.

11. OBTAIN ADDITIONAL LEADS:

a. Determine if the witness knows any other person that might have knowledge of the same incident. Obtain names, addresses, if possible, telephone number of these persons.

b. Determine if the witness know any other person or persons that were present in the area of the incident and get a complete description of these persons.

12. OBTAIN A SWORN DECLARATION, SIGNED BY THE WITNESS.

13. ASSURE THE WITNESS THAT THE INFORMATION THAT HE HAS BROUGHT WILL BE KEPT IN STRICT CONFIDENTIALITY AND THAT HE WILL NOT DISCUSS IT WITH ANYONE ELSE.

14. MAKE ARRANGEMENTS FOR ANOTHER CONTACT OR INTERVIEW IN THE FUTURE WITH THE WITNESS.

a. Advise the witness that you may need to contact him again.

b. Obtain address and telephone number of the witness and determine where you may be in contact with him if you cannot find him at home.

c. Determine if there is any hour in which the witness may not be available for an interview.

15. CLOSE THE INTERVIEW:

a. Explain to the witness that the interview that was just over is considered as an official matter of the government and that he must not discuss it with anyone.

b. Bid the witness goodbye.

16. MAKE THE Review OF FILES.

17. WRITE THE NECESSARY REPORTS.

CHAPTER XIII

PERSONAL INTERVIEW WITH THE SUBJECT

INTRODUCTION:

An interview of the SUBJECT takes place after having completed an history investigation. The office of personal security provides us a preliminary sheet (see example #1), which indicates the purpose of the interview, the type of interview or investigation that is taking place, leads we must follow or develop, history information of the SUBJECT (person to be interviewed), and other special instructions.

GENERAL FACTS:

A. The first thing we must do upon receiving the preliminary sheet is to read it and study it carefully.

The following is the order in which we must carry out the preparation and how to conduct the interview of the SUBJECT:

1. Determine if the information in the preliminary sheet is a valid requirement. To do that, we must:

a. Verify if the preliminary sheet has a pardon date.

b. Look up in the sheet, the identification of the unit that sent the same, the name of the person who signed it and if such person is authorized.

2. Identify the requirements of the interview:

a. Determine what <u>type of interview</u> will take place.

[page missing in original document]

e. Use or abuse of drugs.

f. Abnormal sexual contact.

g. Criminal behavior.

h. Hostage situation.

i. Security matters.

c. Subject interview, in complaint style:

1. This type of interview allows the person to deny, tone down or explain any accusation or allegation against him.

2. These interviews take place to respond to the requirements of the preliminary sheet.

3. These interviews are required when information is obtained that the SUBJECT participates in, or is in a position which he is exposed to blackmail or coercion to participate in:

a. Sabotage
b. Espionage
c. Treason
d. Insurrection
e. Subversive activities

3. Review the personal file of the SUBJECT to identify areas or affairs that will develop during the interview.

4. Develop questions that will be used during the interview:

a. EIA/ES [missing translation]: For these interviews use the subject's HP [missing translation] and obtain the areas (affairs) to be develop during the interview.

b. Interviews about specific affairs/and complaints: Use the preliminary sheet and the subject's file to develop the questions that could fulfill the requirements.

c. Use the basic interrogative words: who, what, when, why, where, and how. Make sure that all areas of interest are exploited.

5. Make arrangements for the interview:

a. Call the SUBJECT to arrange a date.

b. Try to find someone that could act as witness during the interview, if necessary.

6. Select and prepare the interview place:

a. Select a room that provides privacy and eliminates distractions during the interview.

b. Select a room that allows the interviewer to control the physical environment.

c. Select a room where you could keep a nice temperature during the interview.

d. Arrange the furniture in the room. The furniture must be just a small table, and three chairs.

e. Select a room that does not have a telephone and if it does, lift the receiver

f. Install and test recording equipment.

7. Greet and Identify the SUBJECT:

a. Greet the SUBJECT in a professional manner and try to win his trust.

b. Identify the SUBJECT orally and take him to the interview room.

8. During the interview:

a. Verify the SUBJECT'S identity examining his identification card.

b. Identify yourself and your position as representative of military intelligence.

c. If the SUBJECT is of the opposite sex, determine if he/she wishes to have a witness of the same sex present during the interview.

NOTE: IF THE SUBJECT IS OF THE OPPOSITE SEX YOU MAY ADVISE THAT A WITNESS OF THE SAME SEX MAY BE PRESENT DURING THE INTERVIEW.

d. If the SUBJECT is of the opposite sex and wishes to have a witness of the same sex present during the interview we must do the following:

1. Call the witness

2. Introduce the witness and the SUBJECT and explain the responsibility of the witness to the SUBJECT.

e. If the subject does not wish a witness, write this in your Agent's Report.

NOTE: EVEN THOUGH IT IS NOT REALLY A REQUIREMENT TO HAVE A WITNESS OF THE SAME SEX PRESENT DURING THE INTERVIEW, IT IS ADVISABLE TO USE ONE, SINCE WE PROTECT OURSELVES FROM BEING ACCUSED BY THE SUBJECT OF USING ABUSE, COERCION AND THREATS.

f. Inform the SUBJECT of the purpose of the interview.

g. Ask the SUBJECT if he will allow to use a tape recorder during the interview. Explain that the tape recorder will help you in preparing the final report.

h. Turn on the tape recorder only if the SUBJECT has given permission to use it.

i. Advise the SUBJECT of the civil rights that he has: (See example #2)

1. Advise the SUBJECT of his civil rights when:

a. A specific matter of complaint is the subject of the interview.

b. At any time during the interview, the SUBJECT says incriminating things.

2. Make sure that the SUBJECT understands all his rights.

NOTE: IF THE SUBJECT DOES NOT UNDERSTAND HIS RIGHTS, DETERMINE WHAT HE DOES NOT UNDERSTAND AND CLARIFY HIS DOUBTS.

NOTE: YOU MUST NOT INTERVIEW THE SUBJECT UNDER ANY CIRCUMSTANCE IF HE DOES NOT UNDERSTAND HIS RIGHTS.

3. Ask the SUBJECT if he does not wish to contact a lawyer.

a. If the SUBJECT wishes to talk with a lawyer, do not continue the interview until he has the opportunity to talk with his lawyer.

b. If the SUBJECT does not have a lawyer, obtain a sworn declaration from the SUBJECT indicating that he wishes to continue the interview.

NOTE: IF THE SUBJECT DECLARES THAT HE DOES NOT WISH TO HAVE A LAWYER BUT THAT HE DOES NOT WANT TO SIGN A SWORN DECLARATION, CONTINUE WITH THE INTERVIEW AND INDICATE THIS IN THE AGENT'S REPORT.

c. After establishing if the SUBJECT wishes or not to have a lawyer, before starting to question, give the SUBJECT the oath to truth. If the SUBJECT refuses to swear ask him if he is willing to continue with the questions.

4. Inform the SUBJECT of the following privacy rights in regards with the interview:

a. The authority you have to carry out the investigation and obtain the information desired.

b. The main purpose of the obtaining such information.

c. How you will use that information.

d. Why it is obligatory or voluntary to give that information.

5. Have the SUBJECT sign a sworn declaration or document that indicates his understanding of these privacy rights in regards with the interview and the search for information.

j. Ask the SUBJECT about information concerning history information.

k. Ask the SUBJECT about the matters under investigation:

a. Use the questions developed during the preparatory phase.

b. Use the control questions, non-pertinent, repeated and follow-up questions.

c. Examine carefully all the new areas presented by the SUBJECT.

d. Follow a logical sequence of questions to avoid overlooking significant themes.

l. Concentrate in recognizing and interpreting the non-verbal communication of the subject.

a. Listen to how the SUBJECT talks. Audio leads include changes in tone, speed of the voice.

b. Be alert of visual leads, such as facial expressions, body position, hand, legs and head movement.

c. Interpret the subject's non-verbal leads with the verbal leads to obtain a clear idea of the real message.

NOTE: EXPLOIT ALL THE DISCREPANCIES IN THE SUBJECT'S ANSWERS UNTIL EVERYTHING IS CLEARED UP.

d. Use your own non-verbal communications to gain and keep the control during the entire interview.

m. Review the entire matter and affairs discussed up to that point during various intervals of an interview.

1. Identify the areas of interest that have not been discussed.

2. Identify and bring up the inconsistencies and discrepancies in his answering to the SUBJECT .

n. Obtain a sworn declaration:

Make the SUBJECT sign a sworn declaration with all the information he brought during the interview.

o. Close the interview. The interview could end by any of the following reasons:

1. The SUBJECT is sick and requires medical attention.

2. You need more interviews to cover all the areas of interest.

3. The SUBJECT refuses to cooperate with you.

4. All the requirements have been met and the SUBJECT has answered all the questions.

5. You lost the initiative and decide to postpone the interview.

p. Use the closing phase to obtain facts that perhaps were not able to discuss during the interview. The SUBJECT perhaps will calm down more when you end the questioning and turn off the tape recorder or put your notebook away. It is possible that he could bring additional information if he believes that you are not going to record or write down.

8. Say goodbye to the SUBJECT.

9. Prepare the reports/corresponding reports necessary.

EXAMPLE #1

PRELIMINARY SHEET FOR SUBJECT INTERVIEW

PRELIMINARY SHEET DATE/START OF THE INVESTIGATION

1. Subject
Name:
Rank, personal identity number:

2. Date

3. Control number

4. Type and purpose of investigation:

5. Leads to be verified:

6. PAST HISTORY INFORMATION:

7. SPECIAL INSTRUCTIONS:

7. Agency requesting investigation¦Agency preparing investigation

OFFICE	OFFICE
ADDRESS	ADDRESS
SIGNATURE (AUTHORIZATION)	SIGNATURE (AUTHORIZATION)
NAME OF AUTHORIZED PERSON	NAME OF AUTHORIZED PERSON
ADDITIONAL DOCUMENTS ENCLOSED	ADDITIONAL DOCUMENTS ENCLOSED

EXAMPLE # 1 CONTINUED
PRELIMINARY SHEET FOR SUBJECT INTERVIEW

PRELIMINARY SHEET DATE/START OF INVESTIGATION

1. SUBJECT QUINTANILLA, Roberto A. CPT, PPP-00-000 Chalatenango, 10 Dec. 54	2. DATE: May 15, 1988 3. CONTROL NUMBER

4. TYPE AND PURPOSE OF INVESTIGATION:

INVESTIGATION TO DETERMINE IF THE PERSON IS STILL SUITABLE TO HAVE ACCESS TO CLASSIFIED INFORMATION. The SUBJECT at present is assigned to the 4th Infantry Brigade and has access to classified information up to the level SECRET.

5. LEADS TO BE VERIFIED:

Interview Mr. Quintanilla to give him the opportunity to deny, mitigate, or explain the negative information that was obtained during the present investigation.

6. INFORMATION ABOUT PAST HISTORY:
(See the SUBJECT'S personal history)

7. SPECIAL INSTRUCTIONS:

a. Determine the circumstances of subject's arrest by the National Police on 9 April 1980, for driving a vehicle while intoxicated.

b. Determine the financial stability of the SUBJECT.

c. Determine how much he participates in extramarital relationships.

d. Determine if the SUBJECT has used, owned, or traffic illegal drugs including marihuana and hashish.

e. Determine his present and past use of alcoholic beverages.

f. Determine the SUBJECT'S mental and emotional stability.

g. Inform the SUBJECT of his legal rights.

h. Carry out the interview under the SUBJECT'S oath.

i. Send a copy of the interview report to our offices not later than 30 May 1988.

7. Agency requesting investigation¦Agency preparing investigation

OFFICE OFFICE

ADDRESS ADDRESS

SIGNATURE (AUTHORIZATION) SIGNATURE (AUTHORIZATION)

NAME OF AUTHORIZED PERSON NAME OF AUTHORIZED PERSON

ADDITIONAL DOCUMENTS ENCLOSED ADDITIONAL DOCUMENTS ENCLOSED

EXAMPLE #2

HOW TO INFORM THE SUBJECT OF HIS LEGAL RIGHTS

NOTE: THE LEGAL RIGHTS OF A SUBJECT ARE INFORMED IN THE FOLLOWING MANNER:

1. "BEFORE STARTING TO MAKE QUESTION, YOU MUST UNDERSTAND HIS LEGAL RIGHTS".

a. "You are not under obligation to answer my questions or anything else".

b. "Anything you say or do could be used against you in a court or criminal court of law".

c. "You have the right to talk privately with a lawyer before, during and after an interview. You also have the right to have a lawyer present during the interview. Although you will have to make your own arrangements to obtain a lawyer, and this will not be at any cost to the national government.

d. "If you decide to discuss the charges under investigation, with or without a lawyer present, you have the right to finish the interview at any time, or to take privately with your lawyer before continuing to answer, unless you sign a sworn statement testifying that you do not wish a lawyer".

EXAMPLE #3

SWORN STATEMENT/LEGAL RIGHTS/USE OF LAWYER

____ PLACE OF
INTERVIEW DATE TIME FILE NO.

____
NAME UNIT OR ADDRESS

____
IDENTITY NUMBER RANK

____

THE INVESTIGATOR WHOSE NAME APPEARS IN THIS DECLARATION INFORMED ME THAT HE WORKS IN MILITARY INTELLIGENCE OF THE ARMED FORCES OF EL SALVADOR AND WANTED TO QUESTION ME ABOUT THE FOLLOWING ACCUSATIONS/OFFENSES TO WHICH I AM ACCUSED OR SUSPECT:____

BEFORE STARTING TO QUESTION ME ABOUT THE OFFENSES, HE INFORMED ME THAT I HAVE THE FOLLOWING LEGAL RIGHTS:

1. I DO NOT HAVE TO ANSWER OR SAY ANYTHING
2. EVERYTHING I SAY COULD BE USED AGAINST ME IN A COURT OF LAW.
3. I HAVE THE RIGHT TO SPEAK PRIVATELY TO A LAWYER BEFORE, DURING AND AFTER THE INTERVIEW AND TO HAVE A LAWYER PRESENT DURING THE INTERVIEW. NEVERTHELESS I UNDERSTAND THAT IF I DESIRE A LAWYER PRESENT I HAVE TO PROCURE HIM AND PAY HIM ON MY OWN. THE GOVERNMENT WILL NOT PAY THE EXPENSES.
4. IF I AM NOW WILLING TO ANSWER QUESTIONS UNDER INVESTIGATION, WITH OR WITHOUT A LAWYER PRESENT, I HAVE THE RIGHT TO REFUSE TO ANSWER QUESTIONS OR TO SPEAK PRIVATELY WITH A LAWYER, EVEN WHEN I HAVE DECIDED NOT TO USE A LAWYER

____
COMMENTS:

____
I UNDERSTAND MY RIGHTS MENTIONED ABOVE. I AM WILLING TO DISCUSS THE OFFENSES UNDER INVESTIGATION AND TO MAKE A DECLARATION WITHOUT SPEAKING TO A LAWYER BEFORE AND WITHOUT THE PRESENCE OF A LAWYER DURING THE INTERVIEW.

____
WITNESSES
1. NAME:
2. UNIT:
1. NAME:
2. UNIT:

SIGNATURE OF INTERVIEWEE (SUBJECT)

____
SIGNATURE OF AGENT (INTERVIEWER)

____
SIGNATURE OF INVESTIGATOR

____
INVESTIGATOR'S UNIT

____
I DO NOT WISH TO RELINQUISH MY LEGAL RIGHTS:

________ WISH TO HAVE A LAWYER.

________ DO NOT WITH TO BE INTERVIEWED NOR TO ANSWER ANYTHING.

CHAPTER XIV

INTRODUCTION TO SUBVERSION AND ESPIONAGE AGAINST THE ARMED FORCES (SEAAF)

INTRODUCTION:

The knowledge about subversion and espionage against the Armed Forces (SEAAF) has a very important role for counter intelligence agents. The counter intelligence agent must recognize the weaknesses generally sought by a hostile agent and use these weaknesses to get valuable information about the Armed Forces. When the espionage agent of the counter intelligence does not identify these weaknesses he has lost the first battle which is to avoid the collection of intelligence information. (COUNTER-INTELLIGENCE).

GENERAL FACTS:

a. The term "SEAAF" means subversion and espionage against the Armed Forces. A SEAAF incident or a contact is an effort by a foreign intelligence agent to get information, classified or non-classified, using you as the source to obtain the information.

b. First we must have knowledge of the two key SEAAF words which are espionage and subversion.

1. Espionage. Generally, espionage is the act to obtain, give, transmit, communicate or receive information regarding the national defense with the intent or purpose to believe that this information will be used to harm the national government and to the benefit or advantage of the foreign country. Likewise we must keep in mind the following when we talk about espionage terms:

a. Any person or persons in legal, illegal possession, access or control over or he is receiving information regarding the national defense which the person in possession believes such information could be used to harm the national defense and to the benefit or advantage of a foreign country, voluntarily communicates, transmits, or intents to communicate or transmit such information to any non-authorized person, is guilty of the act of espionage.

b. Any person or persons in charge of having legal possession and control over national defense information who by their own negligence allows the same to be lost, stolen, misplaced, destroyed, or removed from the safekeeping place or gives such information in violation of faith, trust, and responsibility, is guilty of an espionage act.

2. Subversion. Generally, the elements of subversion are:

(a) Actively induce the military and civilian personnel of the defense forces to violate laws, disobey legal orders or rules and behavior regulations or to interrupt military activities.

NOTE: "To actively induce" is defined as advising, alerting or requesting in any manner that causes or intents to cause the acts mentioned above. This includes the distribution or intent to distribute the written material that alerts, advises, or requests.

(b) The voluntary intent to intercept, or diminish the loyalty, moral or discipline of the defense forces.

(c) The subversion acts occur during war time or during peace time.

(d) The subversion includes all the voluntary acts with the intent to harm the interest of the national government and that do not fit the categories of treason, insurrection, sabotage or espionage.

c. Having knowledge of the two SEAAF key words, we must recognize also the importance of the insurrection acts.

1. Insurrection. There are four types of specific activities which are taken place with the intention of overthrowing the government through force or violence are acts of insurrection. These four types are:

(a) Training about the need to overthrow the government.

(b) The publication, sale or distribution of written material plotting or training to overthrow a government.

(c) Organizing a society or group with the purpose of plotting or training to overthrow a government.

(d) Members or initiation members or affiliation with this type of society knowing the purpose of such organization.

d. An agent looks for weaknesses to trap, to see if you could be convinced, bribed, threatened, or trapped in a difficult or embarrassing situation so to make you work for him. He must realize some general weaknesses looked for by an agent. These are:

(1) Doubts, financial problems and bad credit.

(2) A criminal file or present criminal activities.

(3) Homosexuality.

(4) Immoral behavior, past or present.

(5) Abuse of drugs or alcohol.

(6) Marriage infidelity.

(7) Routinely boasts and brags.

(8) Mentally or emotionally unstable.

(9) Going with persons of weak character.

(10) Relatives or foreign friends.

e. SEAAF/SAEDA incidents and situations you must report:

(1) Intents of non-authorized personnel to obtain classified or non-classified information about the facilities, activities, personnel or materiel of the armed forces using questioning techniques, seduction, threats, bribe or trapping a person in an embarrassing or difficult situation by personal contact, direct or indirect or by correspondence.

(2) Intent of non-authorized personnel to obtain classified or non-classified information by photography, observation, collection of material or documents or any other means.

(3) Intent by known persons, suspicious persons or with possible foreign intelligence history or associations. Intent to establish any type of friendship, association or business relationship.

(4) Every incident where members of the defense forces, his relatives, travel by or to a foreign area of special consideration (figure 1) who are exposed to:

(a) Questioning regarding their work.

(b) Provide military information.

(c) Bribe, threats or trapped in a difficult or embarrassing situation of any type so as to cooperate with the foreign intelligence services.

(5) Incidents known, suspicious, or possible acts of espionage that result or resulted in danger to documents, information or classified material.

(6) Other acts by members of the armed forces to involve, intent or consider the communication of classified information, documents or material to a non-authorized person.

(7) Non-official contact by members of the defense force with:
a. Personnel they know or suspect are members of a security service or foreign intelligence.

b. Foreign political or military organization.

c. Any member of the countries mentioned in figure #1.

(8) Official contact with personnel mentioned in paragraph #7 when these persons:

a. Show knowledge or curiosity about members of the defense forces.

b. Intent to obtain classified or non-classified information from a member of the defense forces.

c. Intent to establish any type of friendship or business relationship with members of the defense forces outside the official tasks of the defense forces.

(9) Information regarding with international terrorism plans which present a direct threat to personnel, activities, facilities or material.

(10) Known acts or suspicious acts to harm or destroy property of the armed forces by sabotage acts.

f. What you must do if you suspect to have come in contact or someone made contact to obtain information:

(1) Do not deny or accept to cooperate. Ask for some time to think about the proposition.

(2) Remember the person's details. Try to remember things as the description of the person, the place and circumstances of the meeting, identification or description of the vehicle.

NOTE: Do not try to ask the suspect for more information or suggest another meeting in the future. This, may surprise the agent.

(3) Report the contact to the counter intelligence agency. If you cannot contact them, contact the S2 or an intelligence official and tell them about the details of the contact. If you are travelling to another country or abroad, report the contact to the closest consulate of your country or to the office of the Defense (military) Attache.

(4) Do not investigate the matter by your own efforts. Let the investigation up to the qualified counter intelligence agents. Do not tell the contact events to anyone except the departments mentioned above.

Figure 1

GEOGRAPHIC AREAS OF SPECIFIC CONSIDERATION

Afghanistan
Albania
Angola
Bulgaria
Cambodia
Republic of China and its adjacent islands
Cuba
Czechoslovakia
Ethiopia
German Democratic Republic (Communist Germany)
Hungary
Iran
Iraq
Laos
Lebanon
Arab Republic of Libya
North Korea and adjacent demilitarized zones
Nicaragua
Republic of Mongolia
Poland
Democratic Republic of Yemen
Romania
Soviet Sector of Berlin
Syria
Soviet Union
Vietnam
Yugoslavia

CHAPTER XV

INSURRECTION AND ESPIONAGE INTERVIEWS AGAINST THE ARMED FORCES (SEAAF)

INTRODUCTION:

In criminal cases, the identity and the capture of the person is the main objective. In espionage cases the identity of the person is only the first step. The most important thing is the knowledge of his contacts, objectives, information sources and communication methods. The capture and public news of the incident must be the last resource used by the counter intelligence agencies. It is better to identify these persons, what they are doing, and stop the movement of their efforts than to expose them to the public and then try to find out who are their successors.

GENERAL FACTS:

A. Receiving the source.

1. The counter intelligence agent must be professional and courteous with the source.

2. Identify yourself and show your badge.

3. Obtain identification facts about the source.

NOTE: Establish harmony, be friendly and alert, this will help the source to feel confident. Once the harmony has been established with the source, you must be able to hold this confidence during the interview.

4. Determine the purpose and intention of the source.

a. An unscheduled source is a person who comes to a counter intelligence agency to offer information he believes is of interest to military intelligence.

b. The information the source provides must fall within the intentions of SEAAF.

5. Once you obtain the identify data from the source you must start the review of files to:

a. Determine if the source appears in the nuisance files.

b. Determine if the Military Police or other agencies have information about the source.

6. If the review of files reveal that the source is in the nuisance files you must:

a. Thank the source for the information.

b. Close the interview and say goodbye to the source.

7. If the files do not have information about the source, continue the interview.

B. Carry out the interview.

1. First ask permission to the source to use a tape recorder to record the content of the interview. Explain that the tape recorder will help you to prepare the final report as a verbal transcription which the source will have the opportunity to review, correct and sign.

2. Turn on the tape recorder "only" if the source agrees to let you use it.

3. Give the source the oath of truth.

4. Have the source tell you the incident.

a. Encourage the source to tell you the incident in their own words.

b. Be alert and listen to the source and take mental notes of important points to explore these points during the review of the incident with the source.

c. DO NOT write notes while the story of the incident is told.

d. DO NOT interrupt the source while telling the incident.

NOTE: If the source goes off the incident theme he is telling, tactfully make the source return to the main theme.

NOTE: If during the interview the source tells you information outside your jurisdiction, ask the source to go to the appropriate agency. If the source does not wish to go to that agency, continue the interview and collect the information and send it to the proper agency.

C. Carrying out the review of the incident.

1. Assure the source that the information will be kept in strict confidentiality.

2. Review the incident with the source point by point to clarify discrepancies, contradictions, and holes in the information.

3. Write with precision the additional sources.

D. Obtain history information about the source to help you evaluate the information of the source. The history information must include:

1. Identify
2. Date and place of birth
3. Citizenship
4. Addresses (past and present)
5. Occupation
6. Reasons that motivated the source to provide information

E. Develop secondary information. Frequently the information and the source's history could indicate that he could have more significant information and it could be of value or interest to military intelligence.

F. Obtain a sworn declaration.

G. Advice the source that the interview has an official nature and that he must not tell about the incident or nature of the incident to any other person.

H. Closing the interview.

1. Notify the source that the investigation could require a subsequent interview and new contacts with him.

2. Make arrangements to have new contact with the source.

3. Again notify the source about the official nature of the interview.

4. Close the interview in a friendly note.

5. Exit or say goodbye to the source.

I. Start the evaluation of the incident to make sure that it is in your jurisdiction.

J. Prepare the appropriate reports.

1. Prepare an initial report for SEAAF.

NOTE: Make an effort to send a detailed complete report. If a detailed report takes much time, submit an intermediate report with the available information. Afterwards submit the complete report.

2. Classify the SEAAF report according to the Normal Operation Procedures.

NOTE: All SEAAF reports will receive limited distribution.

3. Write down the unit that will receive the SEAAF report.

4. Write down the unit that sent the report.

5. Write down the instructions to send the report.

NOTE: All the SEAAF reports require one of the following sending instructions: "Required Night Actions" or "Hand during the first hours of the day".

6. Complete paragraph A and 1-6 of the SEAAF report.

a. Write down the references in A.

b. Write down the date of the incident in paragraph 1.

c. Write down the place of the incident in paragraph 2.

d. Write down the following information from all the involved persons in paragraph 3:

1. Complete name (father's last name, mother's last name, first name and initial)

2. Date of birth

3. Place of birth

4. Identity card

5. Unit assignation

6. Position

7. Day when separated from the Armed Forces

8. Type of access to classified information

e. Write down in the subsequent paragraphs to paragraph 3:

1. All the sources

2. All the witnesses

3. All persons who have knowledge about the SEAAF incident.

NOTE: If there is more than one person written down in any of the categories mentioned above, write down as #1, #2, etc. (Example: Source 1, Source 2).

NOTE: If the data identification from the witnesses or suspects are not known, write down a physical description available.

4. The description must include:

a. Age
b. Sex
c. Nationality/citizenship
d. Complexion
f. Height
g. Weight
i. Hair color
j. Eye color
k. Appearance
l. Physical built
m. Outstanding characteristics.

f. Write down in paragraph 4, a detailed description of the incident as described by the source(s). Start the paragraph with details in regard to as how the source came to the attention of your agency.

g. In paragraph 5, write down all actions taken, such as review of files or interviews.

NOTE: You will not carry out more actions except as directed by a proper higher agency.

h. In paragraph 8, write down any commentary or pertinent recommendation about the source, suspect or the incident.

K. If applicable prepare the Agent Report with the appropriate exhibits.

1. Send copy or the original and a copy directly to the appropriate higher agency.

2. Send copy of the information, when instructed by the higher investigation elements to the chain of command.

3. Do not do anything else, nor spread information unless it is addressed to the appropriate higher agency.

CLASSIFICATION
REPORT ABOUT INCIDENTS

PAGE_____FROM_____ DATE AND TIME_________PRECEDENT_________________

FROM:

TO:

INFO:

INSTRUCTIONS FOR SENDING:

(CLASSIFICATION)

TITLE OF REPORT:

REFERENCES:

1. ( ) DATE OF INCIDENT:

2. ( ) PLACE OF INCIDENT:

3. ( ) PERSON(S) INVOLVED:

A. ( ) SOURCE(S):

B. ( ) WITNESS(SES):

C. ( ) OTHERS WHO HAVE KNOWLEDGE:

D. ( ) SUSPECT(S):

4. ( ) NARRATION:

5. ( ) ACTIONS TO BE TAKEN:

6. ( ) COMMENTARIES:

7. ( ) POINT OF CONTACT:

NAME,
ORGANIZATION
AND TITLE OF ORIGINATOR

SPECIAL INSTRUCTIONS

NAME, ORG., REVIEWER'S TITLE, TELEPHONE NUMBER

SIGNATURE OF REVIEWER

REVIEW DATE

LN324-91

CLASSIFICATION

( )

REPORT ABOUT INCIDENTS

PAGE______FROM______ DATE AND TIME______PRECEDENT______________

FROM:

TO:

INFO:

____NAME,

ORGANIZATION SPECIAL INSTRUCTIONS
AND TITLE OF ORIGINATOR

____NAME, ORG.,

REVIEWER'S TITLE, TELEPHONE NUMBER

____

SIGNATURE OF REVIEWER REVIEW DATE

____

( )

CHAPTER XVI

ESPIONAGE INVESTIGATIONS

INTRODUCTION:

As counter intelligence special agent you must have specific knowledge of the aspects of an espionage investigation to get security information for a Commander of the Armed Forces responsible for the safety of his command. You as espionage agent must always have in mind that all information must be developed in detail, even though the information is favorable or unfavorable for the SUBJECT.

GENERAL FACTS:

A. Preliminary Sheet (Figure 1).

1. Review the preliminary sheet (PS), found in the control office for the investigation requirements. The PS has specific leads or leads that must be investigated.

a. A PS has collected information during an investigation and could:

(1) Require a development of more investigative leads.

(2) Identify a source that will provide additional information about the case or leads about additional sources that could have information.

b. Areas of interest in the PS are: (Figure 2)

(1) Block 1, SUBJECT: Contains information about the identity of the SUBJECT of the investigation.

(2) Block 4, TYPE AND REASON FOR THE INVESTIGATION: Contains the specific leads or the leads that must be developed. This block also contains information of history and special instructions that will help the special agent in the requirements to develop the leads.

(c) SIGNATURE BLOCK: Make sure that each PS is signed with the signature of the official in charge of the case or authorized person.

(d) BLOCK 8, CONVINCING DOCUMENTS: Identify all convincing documents that are not considered necessary to the development of the required leads.

2. Review the initial report prepared by the personnel of the Armed Forces (AF) involved or who have knowledge of the incident or situation.

NOTE: With the exception of obtaining the initial details of the incident and submitting the priority report, only elements of counter intelligence are authorized to investigate SEAAF cases without the approval of the higher department.

3. Start the espionage investigation when you have the approval from the higher control office, based on the leads originated from various information sources, including:

a. Reports from confidential sources.

b. Reports from other intelligence agencies, security, or police agencies or national guard.

c. OPSEC evaluations, CI technical inspections or reviews.

d. The review of refugees, border crossers, displaced persons, PGE and other similar groups.

e. Routine security personnel investigations.

B. Identify the type of security investigation that you will conduct.

1. Incident investigations

a. These are activities or specific actions.

b. Implications are suspected from acts of espionage.

c. This case will be kept as Type of Incident during the investigation, although, the identity of the person implied will be established at a later date.

2. The Personal SUBJECT investigations.

a. Imply one or more known person.

b. They originate allegations about the specific activities of the person.

c. This case will be kept as personal SUBJECT investigation, although information has developed about an act or specific activity.

3. Investigative jurisdiction. The jurisdiction for the CI section will take place according to the SOP laws.

C. Review of legal statutes which applied to the espionage acts.

1. Espionage - Is the act of obtaining, giving, transmitting, communicating or receiving information regarding the national defense with the intention or reason to believe that the information is going to be used to harm a national government or for the benefit or advantage of a foreign country.

a. Any person or persons with legal or illegal possession, access, control over, has been given confidential information regarding the national defense, which the person in possession has reason to believe the information could be used to harm the national defense and for the benefit or advantage of a foreign country, voluntarily communicates, transmits, or tries to communicate, or transmit this information, to any person who is not authorized to receive it, is guilty of an espionage act.

b. Any person or persons in charge, or in legal possession and control over national defense information, who by negligence allows the same to be lost, stolen, displaced, destroyed, or removed from the place of safekeeping, or gives this information in violation of faith and trust, is guilty of a espionage act.

D. Review the operative methods (OM) of the hostile intelligence agents regarding the activities of the espionage acts.

1. Review the types of hostile operations.

a. Legal Operations. Involve espionage networks which are controlled by a representative from the foreign country who is official charge and is sanctioned by the host country. Frequently, the person possibly has diplomatic immunity, and is not subject to inspections, detentions, or trials for ilegal activities committed.

b. Ilegal Operations. Involve espionage networks that are not in direct contact or relations with the foreign country. Most of these persons are native of the country or of another country. Ilegal operations are more difficult to detect and have the advantage that the operation is continued during war time or in countries that do not have diplomatic relations.

2. Review the control methods of the hostile intelligence.

a. The centralized control procedures require approval from the central headquarters from all the espionage activities. Many countries for security reason regarding the espionage activities have a central control point.

b. The internal control method. Involve operations conducted totally within the host country. All hostile agents are controlled by a general headquarter or by a residence that has been established in the same country. This method is the most outstanding in the external method.

c. The external control method. Involve operations conducted within the host country controlled by another country. This is the safest method to control personnel.

3. Review the type of hostile agents used in a hostile operation.

a. Penetrating Agents have direct access to the information required by the hostile country.

b. Recruited agents in massive form are badly trained and belong to echelon of low category; these agents are infiltrated within the country in great numbers when there are favorable opportunities within that country.

c. Confusion agents are used to deceive the intelligence agencies to waste their efforts in useless investigations.

d. Provoking agents are used to provoke the intelligence agencies to take inappropriate actions for their disadvantage.

e. Sleeping agents are kept inactive for a long time until the hostile country has a mission for them.

4. Review the espionage network used by the hostile country.

a. The single system of agents involves collective intelligence efforts from a person. These agents operate only with the support of the administrative personnel, but only one person is involved in the collective operations.

b. The echelon system are networks that provide security when great number of agents are being used in operation. Only the leader of the network knows the identities of all the members of the network. Contact is initiated only by the higher echelon and code names are normally used. There is no lateral contact because the members of the network do not know each other.

c. The cell system could be simple or complex depending in the number of agents that each cell has. The members of a cell know the identities and the places of each member involved in espionage acts. They have the liberty of coming in contact with each other and as minimum a member of a cell keeps contact with the supervisor. It may or may not be that they have arrangements for unilateral contacts.

d. The echelon network could degenerate in emergencies in a cell type system. Unilateral contact could develop and a member of a segment could be instructed to establish contact with members of another segment.

NOTE: Most of the hostile intelligence services use more than one espionage network to cover or operate in the same area.

5. Review the hostile recruitment methods

a. Acquisition techniques are used to find a person who has been coerced or made to accept recruitment by force.

b. The analysis of sources/potential recruits makes a detailed study of the files and information of past history to identify the potential the person has as agent and his reactions to contacts or possible methods of contact. The motivation of the recruitment also is determined (ideology, money, coercion and selfishness).

c. The recruitment by contact is used to obtain contact with the person and through him obtain his cooperation and involve him in espionage acts. The contact could occur in the person's own country or while the person is traveling in a communist country. The customary way of hostile agents is to allow another person to make the contact and not to involve the agents that did the consecutive process and the analytical steps.

NOTE: The "Small Hook" is the favorite method used by the hostile intelligence service to prepare the potential agent. In this method, the subject is requested to provide innocent information and material of no value to intelligence or classification.

6. Review of the hostile camouflage method.

a. The natural camouflage is the way of legal residence or entry to a country, the use of a real name frequently, occupation or legal ways. The local persons who are recruited normally operate under the natural camouflage because they have established in the community and are employed in the country.

b. The artificial camouflage involves the fabrication of history and position of an agent and the falsification of identification documents in a way that matches the fabrication of history and camouflage history.

7. Review the hostile communication method.

a. Conferences are normally kept to the minimum, but when used, these conferences take place in public areas so as not to arouse the public curiosity.

b. Official messengers are used to transport information to the control official. Diplomatic bags are considered as the safest method to carry material obtained for espionage acts.

c. The post is used to carry information, using codes, secret writing and microfiche.

d. Radios or communications systems are mainly used during operations in war time, but instructions could be transmitted to agents using lateral communication systems at any time such as CB radios or Motorola. The communications through cryptographic systems are used to transmit messages in a safe way.

e. "Mail drops" are hidden secret places used to transmit or safekeep information and material. Most of the services of hostile intelligence put considerable emphasis in the use of "mail drops".

NOTE: Always keep in mind that mail drops could be done by a middlemen and moved to another mail drop to provide necessary security to the controlling officer.

8. Review the Financing Method for espionage activities.

a. Limited or unlimited resources are normally available for espionage operations to the hostile agent.

b. The financial resources will come from the hostile country.

c. The financial resources will be obtained by organizations or hidden business.

d. The financial resources will we obtained by ilegal activities (black market, drugs, etc).

e. The financial resources or money of the target country are transferred to the country by diplomatic bags, official messengers, or by hostile agents.

f. Bank accounts are established in the target country for the access of the agent.

E. Prepare an interrogatory plan (Figure 2)

NOTE: Depending on the type of investigation that will be conducted, the available time, the investigation plan could require only a mental study, or could be a written formal document requiring approval previous to the continuation of the investigation.

1. Plan an investigative agenda detailed for each step of the operation to:

a. Define the requirements of the information.

b. Define the pertinent aspects to be considered.

c. Prevent unnecessary investigative efforts.

2. When the plan develops, consider:

a. The reason or purpose for the investigation.

b. The assigned phases of investigation.

c. The investigation type (open, covered).

d. Priority and suspension time.

e. The restrictions or special instructions.

f. A definition of the problem.

g. The methods and sources that could be used (review of files, interviews, etc.)

NOTE: There is no fixed procedure that could be recommended for treatment of an espionage investigation. One must determine the specific method to each individual case based upon the circumstances of the case.

h. The coordination requirements.

3. Update the investigation plan.

a. When new data is discovered.

b. As a result of continuous analysis.

F. Conduct an investigation of the incident based upon the type, if appropriate.

1. Go to the incident's place.

2. Protect and safeguard the incident place giving appropriate orders and isolating the place physically. All non-authorized persons must be taken out of the place.

3. Find out the circumstances of the incident by visual observation to determine the investigative approach that will be most appropriate.

4. Identify and segregate the witnesses.

5. Obtain photographs of the place, if required, provide a series of photographs to give the maximum amount of useful information and to help the reviewer to understand what had happened.

6. Search the place and collect evidence, if appropriate. Evidence is defined as articles or material found in connection with the investigation or that could help establish the identity of the person or circumstances that caused the incident, in general, facts that will help uncover the events.

7. Control the evidence obtained.

G. Coordinate and conduct ties with other investigation agencies. Coordination is a continuous activity during many of the espionage cases.

H. Interview the witnesses.

1. Conduct interviews of witnesses in the place, if appropriate, to obtain all the pertinent information.

2. During investigations of the subject, conduct interviews of all the witnesses who could have pertinent information or knowledge of the case.

NOTE: The most time-consuming part of the investigation is the interview, because through the interview we obtain the greatest part of the information sources.

I. Conduct the review of files.

J. During investigations of incident type, it will be desirable to make contact with the confidential sources for any information that comes to your attention.

NOTE: Information regarding the espionage incidents or the present espionage investigations will be limited only to few persons and only to persons who need to know the information.

K. Conduct the investigative analysis of the facts of the case. Although, an investigation is basically a collection of facts, the secondary function is also important; the analysis of the facts. The analysis is established in the review and comparison of facts from the case to develop a hypothesis and come up with conclusions regarding the identity of the suspects, circumstances surrounding the incident, and future actions.

NOTE: There are no established procedures to analyze the information from the case to come up with a solution. One method could work as well as another method. All must include the basic function of review, comparison, and hypothesis.

1. Review all information available of the case.

a. Placement and correlation of all information.

b. Examine the information to identify the pertinent facts.

c. Determine the dependability of the information.

d. Determine the truth of the information.

2. Compare the information already known. (Figure 6)

a. Compare the available information with the legal espionage elements.

(1) Identify the information that supports or show the legal espionage elements.

(2) Identify the holes in the information that could be completed with further investigations.

b. Compare the information obtained from witnesses to the information from other witnesses or sources.

c. Identify the possible suspects by comparison of the information.

(1) Identify persons with connection to the incident.

(2) Identify the "opportunity" for possible suspects. ("Opportunity"--the physical possibility that a suspects has of committing espionage acts).

(3) Develop information to prove the motive of each suspect.

(4) Develop information that proves the intent of each suspect.

(5) Develop all the circumstantial evidences and associations of each suspect.

NOTE: In cases of personal subject, the suspect, or possible suspect, is identified therefore. Therefore all efforts are directed to identify his connections in espionage acts, his opportunities, motives, and intents. Show all information and evidence in terms of elements of required evidences to support the charges.

3. Show one or more hypotheses. Hypotheses are theories that explain the facts and that could be examined in later investigations. The best hypotheses are selected to resolve the problem between the information available.

a. Apply inductive or deductive reasoning to show the hypotheses.

(1) Inductive reasoning involves moving the specific and the general. Develop generalities, from observations that explain the relationship between events under examination.

(2) Deductive reasoning involves procedures from general to specific. Starting with the general theory and applying it to the particular incident to determine the truth contained in the theory of the incident.

NOTE: In both processes, the steps must follow a logical manner point by point.

b. If you come to a point where the deductive reasoning is not productive, consider using the intuition. Intuition is the quick, unexpected act which clarifies a problem when the logical process and experimentation has stopped. Intuition must not be ignored, particularly in difficult cases where little progress is evident.

c. Put your hypothesis to a test of considerations of probability, additional information of the witnesses and other known facts.

d. Eliminate various possibilities systematically considering each hypothesis between:

(1) The opportunity

(2) The motive

(3) Observed activities

(4) Corroboration of the alibi.

e. Select the best hypothesis based in the consistency with the known facts and the high degree of probability.

f. Examine the hypothesis objectively.

g. Modify and refute the hypothesis if contradictions to the evidence are discovered.

4. Determine the direction of the future investigation activities.

a. Identify future actions that will examine or verify the selection of the hypothesis.

b. Ask approval from the higher control office to complete the identified actions.

L. Conduct vigilance, if appropriate.

M. Conduct interviews of the SUBJECT, if appropriate.

N. Conduct interrogations of the SUBJECT, if appropriate.

O. Prepare the appropriate reports.

P. Consider an investigation successful when:

1. All information and pertinent material or allegations from the case are discovered.

2. The physical evidence available is completely handled.

3. All witnesses were appropriately interviewed.

4. The suspect, if he allows, is interrogated in an effective way.

5. The report of the case was understood, clear and detailed.

EXAMPLE #1

PRELIMINARY SHEET

PRELIMINARY SHEET DATE/START OF INVESTIGATION

1. SUBJECT
   NAME:
IDENTITY BADGE:
PLACE/DATE OF BIRTH:

2. DATE
   RANK, RANK NUMBER
3. CONTROL NUMBER:

4. TYPE AND PURPOSE OF INVESTIGATION:

5. LEADS TO BE VERIFIED:

6. INFORMATION FROM HISTORY:

7. SPECIAL INSTRUCTIONS:

7. AGENCY

REQUESTING INFORMATION	AGENCY PREPARING REPORT
OFFICE	OFFICE
SIGNATURE (AUTHORIZATION)	SIGNATURE (AUTHORIZATION)
PERSON'S NAME	NAME OF AUTHORIZED PERSON
ADDITIONAL DOCUMENTS ENCLOSED	ADDITIONAL DOCUMENTS ENCLOSED

EXAMPLE #2
INVESTIGATIVE PLAN

1. REASON FOR INVESTIGATION:

2. TYPE OF INVESTIGATION: LIMITED

3. INVESTIGATION WILL BE CONDUCTED: DISCRETELY (Safety will be the main factor during the investigation).

4. PRIORITY:

5. SPECIAL INSTRUCTIONS:

   a.

   b.

6. INFORMATION GIVEN:

7. SEQUENCE OF INVESTIGATION:

   a. Conduct review of local files.

   b. Examine the subject's military and medical files.

   c. Interview the following persons:

      (1) Carry out the review the neighborhoods

      (2) Carry out the review of the financial or credit reports.

NOTE: The plan mentioned above must have flexibility, it is only a guide. Each case must be treated individually. Your plan could be similar, shorter or longer, but this will depend upon the requirements dictated in the Preliminary sheet.

CHAPTER XVII

SABOTAGE INVESTIGATION

INTRODUCTION:

To understand the importance of a sabotage investigation you must always think that the sabotage act is the intent to cause harm, intercept, or obstruct by the desire to cause harm or destroy or intent to destroy material, installations, or utilities with regards to the national defense.

GENERAL FACTS:

A. IDENTIFY THE INVESTIGATION REQUIREMENTS:

1. Use various reports from other agencies to identify the requirements so that the counter intelligence elements could start an investigation of the sabotage act. These reports could be found in the following agencies:

a. Military police

b. Criminal Investigation Divisions

c. Local Civil Authorities

d. The superior authority/supervisor in charge of the facility where the sabotage occurred.

e. Confidential sources that could testify that a particular incident was indeed a sabotage act.

2. Review the Preliminary Sheet (PS), prepared to be distributed by the Central Intelligence Office, to identify the investigative requirements:

a. The PS has information collected during an investigation that may:

(1) Require further investigation and development.

FIGURE/EXAMPLE #1

PRELIMINARY SHEET

PRELIMINARY
SHEET DATE INVESTIGATION STARTED

1. SUBJECT/THEME 2. DATE

3. CONTROL OR FILE NUMBER

4. TYPE AND
REASON FOR INVESTIGATION

7. AGENCY REQUESTING	8. AGENCY PREPARING REPORT
OFFICE	OFFICE
ADDRESS	ADDRESS
FOR G2 ACTION	FOR G2 ACTION (IM)
AUTHORIZED SIGNATURE	AUTHORIZED SIGNATURE
NAME AND RANK	NAME AND RANK
8. CONVINCING DOCUMENTS	CONVINCING DOCUMENTS

4. To condemn a person for an act of sabotage during peace time, you have to prove that he had tried to cause harm described above. In war time it is sufficient to prove that the person had knowledge that his act will affect the "war effort".

5. If more than one person conspires to carry out a sabotage act and one of them is captured while carrying out the plans of the act, all could be accused and condemned for the sabotage act.

C. DETERMINE THE TYPE OF SABOTAGE INVESTIGATION THAT WILL TAKE PLACE:

1. PASSIVE SABOTAGE: This type of sabotage involves the passive resistance of the population and it could be local or at national level. The passive sabotage is not so organized so that persons or groups are assigned specific missions: nevertheless, the population reaction is the result of propaganda, well organized propaganda by a subversive group that is well organized. In other words, the passive sabotage is when a population locally or nationally has been convinced by a propaganda group to carry out or to allow the acts previously described that could be classified as sabotage acts.

2. ACTIVE SABOTAGE: This type of sabotage is characterized by violent sudden actions with visible results and which commonly turn into conflicts with military forces. Within this category, we found the following physical forms of sabotage:

a. Fire sabotage: Is when combustible materials are used to cause fires and destroy government properties. This is normally considered as an act of vandalism or a common criminal act.

(1) This act changes from vandalism to sabotage when it is proven that it took place with the purpose of affecting the national defense, the war or the war effort.

b. Explosive sabotage:

(1) In this type of sabotage explosives are used to destroy or neutralize targets that are resistant to fires and to obtain the maximum quantity of destruction at the minimum time.

(2) Targets that are sensitive to explosive sabotage are:

(a) Bridges
(b) Tunnels
(c) Railroads
(d) Ships/boats
(e) Heavy equipment
(f) Industrial machinery

c. Mechanical sabotage:

(1) the mechanical sabotage is easier to maintain since it does not require instruments or special tools, and normally is directed against railroads, ships or industrial facilities.

(2) The mechanical sabotage is normally classified within one of the following categories:

(a) Destroy/break/tear
(b) Inserting materials or abrasive substances such as, sand, soil, etc., into lubricants and vehicle's fuels.
(c) Omission acts. This consist of not doing something so that a mechanical equipment stop working. Not lubricating a motor so as to damage it, not adjusting a mechanical part so that when the motor is turned on it will stop working.
(d) Substituting real parts for fake parts in apparatus or vehicles.
(e) Contamination of lubricants or fuels.

d. Biological, chemical and nuclear sabotage:

(1) The sabotage with biological agents is know as "biological warfare", and is considered as the introduction of living organism and its toxic products in the environment with the purpose of causing death, impede, or harm people, animals or crops.

(2) Sabotage using chemical agents is know as "chemical warfare: and is considered as the introduction of chemicals to the environment to cause death, impede, or harm people, animals or crops.

(3) Sabotage using nuclear weapons, could just with its destructive capacity, cause serious damage or destruction to property, materials and persons.

D. PREPARE AN INVESTIGATION PLAN: (See example #2)

1. Initial plan:

a. Determine the purpose of the investigation.
b. Determine the place of the incident.
c. Determine what official documents are required to travel to the place where the incident took place (passport, visa, etc.)
d. Make arrangements to get these documents.
e. Determine priorities, if any, that exist in regards to the case being investigated.
f. Determine if any restrictions or special instructions are necessary.

2. Modify the investigation plan according to how you could obtain more information.

E. CARRY OUT THE INVESTIGATION:

1. Go to the place where the incident took place.

2. Write down the date and time you arrived to area and the weather conditions.

3. Visually search the area to try to find wounded persons and:

a. Coordinate medical attention.
b. Write down identity of the wounded, so as to possibly question them later.
c. Coordinate transportation of wounded persons to medical facilities.

(FIGURE/EXAMPLE #2)
INVESTIGATION PLAN

1. PURPOSE OF THE INVESTIGATION:

2. TYPE OF INVESTIGATION: Limited

3. THE INVESTIGATION WILL TAKE PLACE IN THE FOLLOWING MANNER:

   (Discretely)

4. PRIORITY: 30 days after having received the preliminary sheet.

5. SPECIAL INSTRUCTIONS:

   a.

   b.

6. INFORMATION PROVIDED:

7. INVESTIGATION SEQUENCE:

   a. Carry out the review of files.

   b. Examine the medical and military files of suspect.

   c. Interview the following persons:

      (1)

      (2)

      (3)

   d. Carry out the investigation of the neighborhood.

   e. Carry out the review of credit bureaus.

NOTE: THE PLAN DESCRIBED ABOVE MUST BE FLEXIBLE AND ITS INTENTION IS ONLY TO BE USED AS A GUIDE. EVERY CASE MUST BE TREATED INDIVIDUALLY. YOUR PLAN COULD BE SIMILAR, SHORTER OR LONGER ACCORDING TO WHAT THEIR OWN REQUIREMENTS.

4. Coordinate work with other investigation agencies that are present in the incident area, or if they should arrive later.

5. Identify and search a road for the medical personnel to use when arriving to the place where there are wounded and/or dead persons.

6. Do not allow the corps to be covered since this could destroy evidence.

7. Protect the area of the incident using persons to maintain the curious passersby away from the area and to avoid that witnesses, suspects and victims destroy evidence.

8. Protect all that could possibly be destroyed by fire, rain or any other thing, such as footprints, etc.

9. Find the possible witnesses in the area.

10. Ask and write down the identity of the witnesses.

11. Separate the possible witnesses and take them outside the incident area.

12. Carry out questioning/preliminary interviews of witnesses to determine:

a. How much knowledge they have of the incident.
b. Movements that the witnesses have done in the incident area.
c. Any tool that the witnesses or other persons have possibly touched.

12. Write down all the pertinent facts:

a. Identify the persons involved or that were involved in the area.
b. Initial impressions or observations.
c. Take photos of the area in all angles.
d. Take photos of the persons in the vicinity of the area.

13. Search the incident area and adjacent areas to collect all evidence using the search patterns more useful in the area.

a. Pay particular attention to fragile traces of evidence that could be destroyed if not collected immediately.

b. Carefully examine all objects or areas where there may be latent fingerprints and make sure that a follow up is done of this fingerprints.

c. Take photos or prepare imprints that could have value as evidence. (Example: shoe prints, or boot prints on the ground could indicate the amount of persons involved in the incident).

d. Treat stains or accumulation of liquids as evidence and write down its place and take photos of them.

e. Treat any tool as evidence until this could be found to the contrary.

14. Collect, mark for identification and process the evidence.

F. Transfer the evidence to the criminal laboratories and proper agencies to evaluate such evidence.

G. Carry out the review of files.

H. Carry out the interviews with "Witnesses" that are necessary:

1. To obtain more information about the incident.

2. To develop new leads and/or sources.

I. Prepare Preliminary Reports, if necessary.

NOTE: THE PRELIMINARY REPORTS ARE PREPARED WHEN THEY ARE REQUIRED BY THE SOP OR IF AN ORDER IS RECEIVED FROM THE HIGH COMMAND.

J. Contact your confidential sources of information.

K. Carry out an analysis of the information in the case to identify the suspect. Even though an investigation is basically a collection of information, the analysis of such information is a secondary function. This analysis is the review and comparison of information obtained to develop a hypothesis and come up with conclusions that could be used in identifying the suspects and determining the circumstances of the incident and future actions.

NOTE: THERE IS NO FIXED PROCEDURE IN THE ANALYSIS OF INFORMATION OF A CASE TO

ARRIVE AT A SOLUTION. ONE METHOD COULD WORK AS WELL AS THE NEXT. NEVERTHELESS, ANY OF THE METHODS USED MUST HAVE THE BASIC FUNCTIONS OF: (REVIEW, COMPARE, AND MAKE A HYPOTHESIS).

1. Review all the information in the case:

a. Arrange in an orderly fashion all the information.
b. Examine the information in detail to identify the pertinent facts.

(1) Determine the dependability of the information.
(2) Determine the truth of the information

2. Compare the information known:

a. Compare the available information with the legal aspects of sabotage.

(1) Identify facts/evidence that support or prove the legal elements of sabotage.

(2) Identify vulnerabilities in the information that could require further investigation.

b. Compare the information obtained from witnesses with such obtained by other witnesses and sources.

c. Identify possible suspects through the information comparison.

(1) Identify such persons that have connection with the incident.
(2) Identify information that supports or proves the "OPPORTUNITY" that possible suspects may have. (Ask yourself: Is it physically possible that the suspect could have committed the act of sabotage?)
(3) Identify information that supports or prove "MOTIVATION" by each suspect.
(4) Identify information that proves "INTENT" by part of the suspects.
(5) Identify all circumstantial or association information related with each suspect.
(6) Evaluate all information and evidence in regards to the test elements required to support the sabotage accusation.

3. Show one or more hypotheses. The most possible hypotheses are selected to solve a problem according to the information and available evidence.

a. Apply deductive and inductive reasoning to show your hypothesis.

(1) Inductive reasoning involves moving from the specific to the general. Develop a generalization of the information being evaluated that could explain the relationship between events under investigation.

(2) Deductive reasoning involves moving from the general to the specific. Start with a general theory and apply it to the particular incident to determine if the truth of the incident is part of the theory.

NOTE: WHEN USING DEDUCTIVE AND INDUCTIVE REASONING, THE MOVEMENT FROM ONE POINT TO ANOTHER MUST BE DONE LOGICALLY.

b. During the study of information to show a hypothesis, the concept of intuition must be considered. Intuition is an internal and sudden solution towards a problem. Intuition frequently clarifies a problem when there is no progress through logic.

c. Submit the hypothesis to probability tests, additional information of other witnesses, and other data already known.

d. Eliminate the possibilities through the systematic comparison of the hypothesis with the following considerations:

(1) Opportunity
(2) Motivation
(3) Observed activities
(4) Corroboration of the suspects' bribes

e. Select the best hypothesis based in the consistency of data compared and the high degree of probability.

f. Test the hypothesis objectively.

g. Modify and/or refute the hypothesis if information to the contrary is found.

4. Determine the requirement/direction of the future investigation activities.

a. Identify what could support or prove the hypothesis selected.

b. Get the approval of the Control Office to initiate actions that have been identified.

L. Carry out the follow up, if necessary.

M. Carry out the personnel interviews if necessary.

N. Carry out a CI interrogation of suspects, when there is suspicion in regards to the identity of a person.

O. Prepare and distribute the required reports.

P. You may consider that the investigation was successful when:

1. All the information and material related to the case has been discovered and developed.

2. The physical evidence available was handled.

3. All the witnesses were interviewed.

4. The suspect was properly interrogated.

5. The case has been reported in a clear, exact and intelligible manner.

CHAPTER XVIII

PREPARING AGENT'S REPORTS

INTRODUCTION:

After the CI agent finishes an investigation or part of the investigation, the following step is to write down all the information in a report, which is known as the Agent's Report. The preparation of this report requires a great effort and skill from the agent. To know how to prepare a good agent's report is one of the requisites and duties of any counter intelligence agent. In this chapter we will discuss all the areas and rules that govern the proper preparation of an agent's report.

GENERAL FACTS:

NOTE: For effects of this chapter we will use as example an agent's report, see the format that appears in EXAMPLE #1.

A. COMPLETE BLOCK #1: (NAME OF SUBJECT OR TITLE OF INCIDENT)

NOTE: Typewrite all the information in this block as close as possible to the left margin and below block #1.

1. THE TITLE BLOCK in this report is always the same that appears in the preliminary sheet (refer to previous examples), or of any pertinent investigative report, with only two exceptions:

a. Change the title block to include alias or any other essential information developed during the investigation.

b. Change the title block to change any error in the preliminary sheet. All changes and corrections will be written down in Section "Agent's Notes" of the report.

2. When there is no preliminary sheet, or any other investigative reports in regards to this case, prepare the title block in the following manner:

(2) Write down the answer to the question "Where" in the second line.

(3) Write down the answer to the question "When" in the third line.

B. Write down the date in which the report was prepared in block #2 (day, month, year).

C. Write the control number in block #3 (CONTROL NUMBER OR FILE NUMBER)

1. If you have a preliminary sheet the name that appears in block #3 of the sheet could be used in this report as well.

D. Complete block #4 (Report of Findings): (SEE FIGURE/EXAMPLE #1)

1. Use this block to write down the information obtained during the investigation. This is the most important part of the Agent's Report and must:

a. Show in detail all the facts that the source brought. Write down as facts as facts and opinions as opinions.

b. It must be pertinent and directly related to the investigation.

c. Be written clearly, orderly and clearly understood to avoid wrong interpretations of facts.

d. Be impartial, and include favorable and unfavorable information developed during the investigation.

e. Be concise and to the point. Describe exactly the activities and attitudes of the SUBJECT. Avoid unclear phrases.

f. Be complete.

2. Normally, write the report:

(1) In narrative style
(2) Using third person (grammatically)
(3) Using the simple past.

3. PRIVACY PHRASES: (SEE FIGURE/EXAMPLE #2)

a. According to Figure #2 select and write down the most appropriate privacy phrase.

b. Write down the phrase in the third line where block #4 starts.

c. Leave 15 spaces where the left margin of the report.

d. This phrase is written entirely in capital letters.

4. DESIGNATION OF PHRASES: (SEE FIGURE EXAMPLE #3)

a. Select the appropriate phrase on Figure #3 and write down in parenthesis according to the description in Figure #1.

b. It is written two spaces under the Privacy Phrase.

5. Start the Introduction paragraph which has the information about the SOURCE, including identity, employment and address.

a. This paragraph starts in the same line of the Designation Phase.

b. In the right margin of the report, allow a blank area of at least five spaces to write down the word (LEAD) if necessary. (A LEAD is any information collected during the investigation that requires further development. It could be a name, address, or whereabouts of a person or organization.

c. Write down the specific information in the Introduction Paragraph according to the type of report. (SEE FIGURE/EXAMPLE #4, TO SEE WHAT INFORMATION COULD BE USED ACCORDING TO THE REPORT TYPE AND IN WHAT ORDER)

d. Write the last name of the SUBJECT in capital letters in the report's text always.

FIGURE/EXAMPLE #1

AGENT REPORT FROM

1. SUBJECT NAME OR TITLE OF INCIDENT RAMIREZ, Juan O. TCC: TORRES, Antonio O. CPT, 000-00-000 FLDN: 9 March 1956, San Salvador, ES	2. DATE 15 May 1988 3. CON. NUMBER

4. REPORT OF FINDINGS:

WRITE HERE THE PRIVACY PHRASE USING CAPITAL LETTERS.

(PHRASE DESIGNATION) Here starts the introduction paragraph under the privacy phrase and in the same line of the designation phase. Allow a space in the right margin to write the word (LEAD) when one comes up during the investigation.

(LEAD)

If there are more than one paragraph allow two spaces between the paragraphs and prepare the first the same as the second.

(RUMORS IDENTIFICATION) Rumor information is written down in a separate paragraph and is indicated with the phrase RUMORS INFORMATION in parenthesis.

AGENT'S NOTES: Here you write down all the notes or commentaries that the agent has in reference to the source or the case. The agent's notes are used only once in the report.

5. NAME AND ORGANIZATION OF AGENT 6. AGENT'S SIGNATURE

FIGURE/EXAMPLE #2

PRIVACY PHRASES

THE SOURCE DID NOT HAVE AN OBJECTION IDENTIFYING HIS IDENTITY TO THE SUBJECT.

THE SOURCE RECEIVED A PROMISE OF CONFIDENTIALITY AS A CONDITION OF HIS COOPERATION WITH OUR INVESTIGATION.

THE INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED IN OFFICIAL FILES FROM THE GOVERNMENT.

THE INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED FROM PUBLIC FILES.

THE INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED FROM MILITARY MEDICAL FILES.

THE INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED IN MILITARY FILES FROM THE PERSONNEL OFFICE.

THE INFORMATION CONTAINED IN THIS REPORT IS OBTAINED FROM CIVIL FILES.

THE INFORMATION CONTAINED IN THIS REPORT IS FINANCIAL INFORMATION AND WILL NOT BE REVEALED TO ANY OTHER AGENCY.

FIGURE/EXAMPLE #3

DESIGNATION PHRASES

(SUSPECT'S INTERROGATION)

(FILE REVIEW OF LOCAL AGENCIES)

(MILITARY SERVICE)

(MEDICAL FILES)

(MILITARY FILES)

(CIVILIAN PERSONNEL FILES)

(CITIZENSHIP)

(BIRTH)

(CREDIT REFERENCE/WRITTEN DOWN)

(CREDIT REFERENCE/DEVELOPMENT)

(PERSONNEL REFERENCE/WRITTEN DOWN)

(PERSONAL REFERENCE/DEVELOPED)

(NEIGHBORHOOD CHECK)

(SUBJECT'S INTERVIEW)

(EMPLOYMENT SUPERVISOR)

(CO-WORKER)

(EMPLOYMENT FILES)

(EDUCATION FILES)

(EDUCATION INTERVIEW)

(DEVELOPMENT/EMPLOYMENT SOURCE)

(DEVELOPMENT/RESIDENCE SOURCE)

(DEVELOPMENT/EDUCATION SOURCE)

(MILITARY COMRADE)

(MILITARY FILES REVIEW)

(MILITARY SUPERVISOR)

(COMMANDER)

(FIRST SERGEANT)

(POLYGRAPH TEST)

e. Use the complete name of the SUBJECT in the first sentence of the introduction paragraph.

6. Complete the rest of the report, writing down all the information about the SUBJECT obtained during the investigation. The exact report format will be determined by the type of report. Below, we list various formats for the different types of reports:

a. INVESTIGATION REPORT OF PERSONNEL SECURITY:

1) Enter the association paragraph which has a complete and concise description between the Source and the SUBJECT.

(a) This paragraph must be answered with the questions in figure #5 as a minimum, which will establish the nature, degree and length of its association. (SEE FIGURE/EXAMPLE #5)

(b) Write down the last name of the SUBJECT the first time it comes up in the association paragraph. After mentioning for the first time, it could be referred to it with the word SUBJECT.

2) Between the history paragraph which contains information of the SUBJECT'S history, such as:

(a) Date and birth place
(b) Family situation/marriage
(c) Military service
(d) Residences
(e) Education
(f) Employment
(g) Associates

NOTE: Information areas that are not covered during the interview could be used to include the first sentence like: (The source could not provide more information about the education, residence, employment of the SUBJECT).

NOTE: The history information must be written down chronologically, that is in the time frame they occurred.

3) Between the LIDMC paragraph, which contains favorable and disfavorable information in regards to loyalty, integrity, discretion, moral and character of the SUBJECT. (This is known as LIDMC) Areas that enter or are discussed in the LIDMC paragraph are:

Sexual moral
Ethics
Honesty
Integrity
Maturity
Discretion
Character
Mental stability
Emotional stability
Betting
Alcoholic beverages
Drugs

Non-prescribed medications
Financial stability
Improper gains
Police agencies
Government overthrow
Deny civil rights
Other organizations
Foreign travels
Friends/foreign friends
Foreign business connections
Loyalty

NOTE: Answer all the questions on the themes mentioned above even though the SUBJECT gives you a negative answer such as (I DON'T KNOW). The negative answers are included in the report in the last sentence, ("THE SOURCE did not provide information about the SUBJECT'S foreign travels").

4) Between the RECOMMENDATION paragraph such as the last paragraph of the personal security investigation report.

(a) This paragraph contains the recommendation from the source in regards to if he recommends that a position of trust and responsibility is given to the SUBJECT.

(b) Use the SUBJECT'S complete name and not the word SUBJECT in the first phrase of the recommendation paragraph.

(c) A source could be give one of four recommendations:

(1) He could decline to recommend him: "The Source refused to give a recommendation in regards to Arturo G. RIVAS, for a job in a position of trust and responsibility since he has only known hin for (8) weeks.

(2) Could give a favorable recommendation: "The Source recommended Arturo G. Rivas for a position of trust and responsibility with the national government".

(3) Could give a non-favorable recommendation: "The Source did not recommend Arturo G. RIVAS for a position of trust and responsibility with the national government due to his dishonesty and lack of integrity. The Source made a sworn declaration and was willing to appear before a hearing or trial in regards to the SUBJECT."

(4) Could give a qualified recommendation: "The Source recommended that Arturo G. RIVAS is considered favorably for a position of trust and responsibility with the national government, under the condition that he (RIVAS) control his drinking habits. The Source made a sworn declaration and was willing to appear before a hearing or trial in regards to the SUBJECT.

b. Files review:

1) The format will depend upon the type of file being reviewed:

(a) The information obtained from the normal files will be presented in a tabulated manner (SEE FIGURE/EXAMPLE #6).

(b) The information was also presented in a narrative manner. (SEE FIGURE/EXAMPLE #6)

(c) A combination of narrative and tabulation could be used. (SEE FIGURE #6).

c. Incident, complaints, or limited investigations:

(1) Write down one or more information paragraphs that describe the clear and complete story.

(2) Present all information in chronological order.

(3) Answer the following questions to develop all the information:

(a) Who
(b) What
(c) Where
(d) When
(e) Why
(f) How

d. When a report is long and there is not enough room in the first page:

(1) Allow at least half inch of space in the lower part of the report and write down (continued) between parentheses on the lower part below the report. (If there is need to include classified information in this report, allow at least one inch of space.

(2) The report could be continued using the same format on the first page with the same information in blocks 1-3 and from 5-6.

7. Write down the Rumors' Information if applicable: (SEE FIGURE/EXAMPLE #1):

a. Use this paragraph when developing rumors or information such as that.
b. When the original source of the information could not be determined.
c. When leads that could verify or deny this information could not be identified.

NOTE: Put the paragraph (Rumors' Information) in the Investigation of Personal Security reports between the LIDMC paragraph and the Association paragraph.

8. Enter the agent's notes paragraph:

a. This paragraph helps officials that review the report to evaluate the information, and call the pertinent discrepancies to attention.

(1) Discuss the reason why a lead was not developed or why a particular lead could not be developed.

(2) Write down facts of your (Agent) personal knowledge that could help to clarify the incident.

(3) Write down the pertinent information from the Source and do not discuss the rest of the report.

(4) From your personal opinion of the SUBJECT, or the information acquired from him, if it is necessary to clarify some doubts. It must be specified that this is only the Agent's opinion.

(5) Discuss any existing discrepancies in the Personal History of the SUBJECT.

(6) Discuss the condition in which the files reviewed were found, if this affects its validity or not.

(7) Explain and discuss any work or phrase that is difficult to understand normally.

(8) Call attention to conflicts or discrepancies in the different stories that come up from the investigation in regards to the same information. Write down your personal opinion about which of the stories you personally think has more validity.

(9) Indicate if any of the sources have the same last name or are related. (Only if it applies in the report).

b. Do not use the Agent's notes to:

(1) Provide much information that is not pertinent to the case.

(2) Point out the minor discrepancies in the Personal History of the SUBJECT.

(4) Describe the difficulty you had to find a source.

(5) Indicate recommendations.

E. COMPLETE BLOCK #5: (NAME AND ADDRESS OF THE ORGANIZATION OF THE SPECIAL AGENT) (SEE FIGURE/EXAMPLE #1)

F. EDIT/REVIEW YOUR REPORT ACCORDING TO THE FOLLOWING RULES:

1. Structure of the sentences and their contents:

a. The sentences must be:
  1) clear
  2) concise
  3) simple
  4) impartial

b. The sentences must not contain:
  1) Local idioms
  2) Vulgar words (Unless you are quoting the SUBJECT'S exact words).

2. The correct use of the work SUBJECT, and the name of the person who is interviewing:

a. Always write the name of the person interviewed in capital letters.

b. The word "SUBJECT" in capital letters could substituted the name of the interviewee, except:

1) In the first sentence of the introduction and recommendation paragraphs.

2) The first time the interviewee is mentioned in the association paragraph.

c. Write in capital letters all the pronouns that are used to refer to the SUBJECT. EXAMPLE: (HE, SHE).

3. The appropriate use of the word "SOURCE":

a. Write down the name of the source normally when it its mentioned in the report, without using capital letters.

b. You may substitute the word "Source" with only the "S" in capital letters when mentioning the source in the report.

c. If you wish to use the pronoun to refer to the Source, write the first letter in capital letters, "He", "She".

4. The appropriate use of the names of other persons mentioned in the report that are not the "SUBJECT or the Source".

a. The first time another person is mentioned in the report, you must completely identify him, including the complete name, employment address, residential address or any manner in which we could contact him.

b. After identifying the other persons for the first time, you could refer to them in the rest of the report using only their last name, unless when two persons have the same last name, then you must identify them with their complete name.

c. If only the last name of the person is known, write down FNU, which means, FIRST NAME UNKNOWN, EXAMPLE (FNU Gonzalez).

d. If you only know the first name of the person, write down LU, which means LAST NAME UNKNOWN, EXAMPLE (Raul LU).

e. Never use FNU, LU, together. If you do not know the name of the person, indicate it in the following manner.

"The SUBJECT was married with a woman, unknown name...".

f. If a source is not sure as to how to spell a name, write down the word "Phonetics" in parenthesis after the name. This means that the name was spelled by sound only.

g. Indicate the maiden names of the women in the following manner. (Maria Gomez, N: Gonzales) This means that the maiden name of Maria is Gonzales.

h. Do not identify the confidential sources by their proper names. Use the numbers or code names only. Do not use phrases in the report that could identify, or help find a confidential source in your reports.

5. CAPITALIZATION: When you are preparing the Agent's report you must follow the following rules in regards to writing words and capital letters. Capitalize:

a. The first word of each sentence.

b. The first letter of the word "Source".

c. The first letter of proper names, places, countries, races, languages, months, and days of the week.

d. All letters of the SUBJECT'S last name.

e. All the words in the PRIVACY PHRASE.

f. The word SUBJECT.

g. All the PHRASES OF DESIGNATION.

h. Al the classifications of security (CONFIDENTIAL, SECRET, ULTRA-SECRET).

i. Pronouns when they are substituted by the SUBJECT'S name (HE, SHE).

j. Names of all the political parties and organizations (Liberal Party).

k. All the titles before the names (Dr., Att., Md.)

l. Titles of rank, office, or profession if accompanied by names, (GONZALES, Raul, JCS, Joint General Staff).

m. Names of regions, locations, or geographic structures, (East, West, North).

n. The names of organizations formally structured and established. (Joint General Staff, Department of National Investigations, National Police, etc.)

o. The names of languages, (English, Spanish, French, etc.).

p. The names of schools, universities, (Santa Maria School, University of El Salvador, etc.)

q. University degrees, (Master in Medicine, Law, etc.)

6. DO NOT CAPITALIZE THE FOLLOWING:

a. Names of studies/courses (mathematics, history, biology, chemistry) except languages (English, Spanish, French, etc.).

b. Descriptive terms to show addresses, (over, below, at left, at right).

7. The use quotation marks " " "

a. Do not use quotation marks to show common nicknames, unless it is used with the full name of the person. (Herman "Babe" Ruth).

b. Do not use quotation marks with names of newspapers and magazines, underline them: (El Diario).

8. Use of commas:

a. Use commas between cities and country, (San Salvador, El Salvador).

b. Use a comma to separate absolute phrases, (Juan Jimenez, the richest man in the world, was arrested yesterday).

9. Underline:

a. Underline words in another language, followed by the translation to Spanish in parenthesis, (He worked at the Post Office (Correo).

b. Underline any information developed during the interview that is different than that which appears in the SUBJECT/TITLE block.

9. The use of short titles:

a. To use short titles means to take the first letter in each name of an organization or theme and to write them in parenthesis, later, the short title could be used in the report:

EXAMPLE: "The Source works in the Joint General Staff of the Armed Forces (JGSAF), of El Salvador (ES).

b. As soon as the short title is established it could be used without the parenthesis. Only use the parenthesis when mentioning the short title for the prist time. EXAMPLE: The Source said that the SUBJECT also worked at JGSAF, ES.

c. The short titles are used for schools, units and military installations.

d. Never use short titles for person's names.

e. Do not use short titles if the phrase will only be used once in the report.

10. Abbreviations:

a. Do not use many abbreviations in your reports.

b. If you use abbreviations, spell out the complete word the first time mentioned in the report, and later use only the abbreviation.

c. Do not abbreviate military ranks if they are mentioned alone without a name, (The man was a captain). You may abbreviate when it is accomplished by a name, (The CPT Ramirez is a good soldier).

d. Never abbreviate the months in the year and use the complete year in your reports, (the 15 May 1988).

11. The use of numbers and numerals:

a. When using numbers from one to nine, spell them out, (one, two, three, four,...nine).

b. From nine on you may use numerals (10, 11, 12, 13, etc.).

c. Use numerals to describe:

(1) Sums of money. The amount does not matter always use numerals.

(2) Numbers in streets in addresses, (50th Street).

(3) Apartment and room numbers.

(4) Temperature degrees, prices, percentages, etc.

d. Do not use numerals:

(1) When starting a sentence, spell out the number, (Four terrorists were captured yesterday).

e. Use the following rules for the military reports:

(1) Use the military form of writing the time (According to your SOP).

(2) The units, companies, squadrons, regiments, etc., could be abbreviated and are not placed in numerical order when mentioned in the report. (He belongs to the 1st Squadron, 2nd Company, Cavalry Regiment).

G. Complete Block #6 (SIGNATURE):

1. Sign your name the same way in which it appears written in block # 5.

2. All reports require an original signature in each page, do not use carbon paper or stamps when signing the report.

H. Mark all the pages of the report with its appropriate classification. (The classification will be selected according to the requirements of your SOP).

I. Send the completed report to the Control Office.

FIGURE/EXAMPLE #4
EXAMPLES OF INFORMATION FOR THE INTRODUCTION PARAGRAPH

1. SOURCE'S INTERVIEW (INVESTIGATION OF HISTORY):

(DESIGNATION PHASE): Interview date; identity of interviewed person (name, occupation, residence, rank, serial number, position); and the place where the interview took place. The reason for the interview, and the association and period of knowledge between the SUBJECT and the interviewer.

2. SOURCE'S INTERVIEW (INVESTIGATION OF THE INCIDENT):

Interview's date; complete identity of the source; interview place, and if necessary, the reason for the interview.

3. FOLLOW-UPS:

Date, length, follow-up type and any information with respect to persons under follow-up (observation); place, and the identity of the persons that are handling the follow-up. If the situation requires the protection of the identity of the persons (without counting the agents), a code reference must be used.

4. SUBJECT INTERVIEWS:

(DESIGNATION OF PHASE); date of the interview, identity of the SUBJECT (complete name, rank, serial number/identity number, position, employment place and residence address and employment place); sworn declaration of truth; interview place; purpose for the interview; notice of legal rights; notice of need to have a written sworn declaration by the SUBJECT.

5. REVIEW OF FILES:

(DESIGNATION PHASE); review date; finding the files, office or any place, name and position of the person who brought access to the files, complete identity of the file (title, page, or any other information that helps in the identification of the file).

CONTINUATION OF FIGURE/EXAMPLE #4

6. SEARCHINGS, SCRUTINIES, SEIZURES:

Date of activity, identification of persons and/or units carrying out such activity; and the authority to carry out this authority. In scrutinies and seizures you need the name of the official that serves as witness. (Normally this person is the SUBJECT'S commander).

7. INVESTIGATIVE INTENTS:

Date of intent, identity of the persons whom they tried to interviewed; identity of persons to whom they talked; reason for which the person was not able to be interviewed; and any other possible lead. The explanation must show that everything possible was done to find the source or the person but it was not possible.

8. CONFIDENTIAL SOURCES:

Sources that have codes for identification purposes will not be identified, neither phrases nor information that could give leads as far as identity or location will be included in the report. The confidential sources will only be mentioned by its code, or designated symbol. To help evaluate the information, the Agent indicates through a phrase the security level the source has. EXAMPLE:

"The Source, who has brought confidential information in the past...

"The Source, who has brought information that has been corroborated partly by other sources.....

"The Source, whose security is unknown, but who has known the SUBJECT during the last five years....

FIGURE/EXAMPLE #5
ASSOCIATION PARAGRAPH

1. The first time they met (were introduced) and the circumstances of such meeting.

2. The last time they met and the circumstances.

3. Type of contact (professional or social, or both).

4. Contact frequency.

5. Closest association period, if any.

6. Moments in which they did not have contact for 31 days or more.

7. Communication between them during the period in which they did not have contact.

8. Communication or correspondence from the date of last contact.

FIGURE/EXAMPLE #6

AGENT REPORT FROM

1. SUBJECT'S NAME OR TITLE OF INCIDENT

2. DATE

RAMIREZ, Juan O.
TCC: TORRES, Antonio O.
CPT, 000-000-000
9 MARCH 1956, San Salvador, ES

15 May 1988

3. CONT. NUMBER

4. REPORT OF FINDINGS:

WRITE HERE THE PRIVACY PHRASE USING CAPITAL LETTERS.

(MEDICAL FILES) El (DATE), Juan O. RAMIREZ'S military medical files at the Military Hospital, San Salvador, El Salvador were reviewed by (rank and Agent's name), Special Agent, Joint General Staff, substantially and revealed the following information:

NAME:

RANK:

SERIAL NUMBER:

UNIT:

DATE OF LAST MEDICAL CHECKUP:

The SUBJECT'S file did not have information that could indicate the ilegal use of drugs or marihuana; abuse of prescription medicines or any other medicines; the chronic use of alcoholic beverages, or mental or nervous disorders. No physical disorder or medicines indicated in the file give any abnormal indications.

5. NAME AND ORGANIZATION OF AGENT

6. SIGNATURE OF AGENT

REPORT FROM

AGENT

1. NAME OF SUBJECT OR TITLE OF INCIDENT 2. DATE

3. CONT. NUMBER

4. REPORT OF FINDINGS:

5. AGENT'S NAME AND ORGANIZATION 6. AGENT'S SIGNATURE

CHAPTER XIX

INVESTIGATION REPORT

INTRODUCTION:

As CI espionage agent you must have the knowledge of how to prepare an investigation report. An investigation report is an accumulation of agent's reports in a concise summary of basic interrogations in which only the facts are written down.

GENERAL FACTS:

NOTE: Example #1 is the format for the investigation report.

A. PREPARE THE REPORT'S HEADING:

1. Write down the date in which the report was prepared in the block "DATE SUBMITTED" in the report.

2. Write down the "focus" information if it applies in this report. This block is pertinent if the report deals with an investigation of history. If this is not an investigation of history, leave this block blank.

3. Write down the category of the case in block "CASE CLASSIFICATION". (Example: Espionage, Sabotage, Subversion, etc).

B. If this is a Personal investigation of a SUBJECT (that is, in which the SUBJECT is known) fill out blocks 1 to 10. If the SUBJECT is not know, enter N/A (Not applicable) in these blocks.

1. Write down the name (last name in capital letters, first name, and initial) of SUBJECT in block #1.

2. Write down the serial number, identity number, of the SUBJECT in block #1.

3. Write down SUBJECT'S race in block #3.

4. Write down the rank, that is military or civilian, in block #4.

5. Write down the branch of the Armed Forces to which the SUBJECT belongs, in block #5.

6. Write down the position that the SUBJECT occupies in block #6.

7. Write down the date of SUBJECT'S date of birth in block #7.

8. Write down the SUBJECT'S place of birth in block #8.

9. Write down the unit or the employment address of SUBJECT in block #9.

10. Write down the SUBJECT'S residential address in block #10.

C. If this is an INCIDENT case (Person or unknown persons), fill out blocks 11 to 15. If this is not an INCIDENT case, write down N/A in these blocks.

1. Write down the incident's title in block #11.
2. Write down the incident's date in block #12.
3. Write down incident's time in block #13.
4. Write down the place where the incident occurred in block #14.
5. Write down the register numbers or serial numbers of any equipment that was involved in the incident in block #15.

D. Complete the Control Section:

1. Write down symbol/control number or the file number in block #16.

2. Write down the name of organizations that are involved in carrying out the investigation in block #17.

3. Write down the name of the control office in block #18.

E. Complete "Investigation Facts" section:

1. Write down the name of the person or organization that requested the report in block #19.

2. Write down the reason for which the investigation is being carried out in block #20.

3. Write down the information about the date of investigation in block #21:

a. Write the date in which the investigation started.

b. Write down the date in which the investigation ended (If it has not ended yet, write down N/A in this space).

F. Write down the "Present Situation of the Case" in block #22:

1. CLOSED: An investigation is indicated as "CLOSED" when there is no need for further investigative activities for the authorities to make a decision upon the case.

2. FINISHED/ELIMINATED: An investigation is considered FINISHED when the investigation has stopped for any reason that is not the conclusion of the case.

3. SUSPENDED: An investigation is considered SUSPENDED when the information obtained is not complete and all the tangible leads have been exhausted, but there is a possibility yet that new information will spring up in the future.

4. PENDING: An investigation is considered PENDING when the investigation is continuous. (or that there are many facts and leads to be resolved and developed yet).

F. Complete the "Synopsis" Section:

NOTE: THE Synopsis IS A SUMMARY, CONCISE, IN PARAGRAPH FORMAT, WRITTEN IN A LOGICAL SEQUENCE OF INVESTIGATIVE ACTIONS, AND ANSWERING TO THE MOST COMPLETE MANNER TO "WHO", "WHAT", "WHEN", "WHERE", "WHY", AND "HOW" OF THE INVESTIGATION. RECOMMENDATIONS, OPINIONS, OR CONCLUSIONS MUST NOT BE INCLUDED IN THIS REPORT. THESE COMMENTARIES MUST BE INCLUDED IN THE TRANSMISSION LETTER OF THE INVESTIGATION REPORT.

1. Margins:

a. Start the report three (3) lines below de black border in the upper part of the Synopsis block.

b. The black border in this report will serve as the left margin of the report.

2. Enumeration of Paragraphs: The paragraphs in the Synopsis Section of this report will not be enumerated.

3. Classification of paragraphs: Each paragraph of the Synopsis will have the Specific Classification of that paragraph at the beginning. This is done by writing the classification of each paragraph in quotes at the start of the paragraph. (Example:

(C) THE STUDENTS WERE......

4. Convincing documents to the report:

a. All convincing documents (or additional documents) to the report will be named in parenthesis within the Synopsis paragraph that these support. For Example if Agent #1's report supports the first paragraph of the Synopsis, you will include something like this within the paragraph: (Agent #1's report).

5. Classification of the report: The report will be classified according to its content, and what is stipulated in the SOP.

G. Continuation pages: If the report could not be finished in the first page, it is continued in another page in blank, using the normal margins according to the SOP.

1. In the upper part of the continuation page, write the Title (Theme), or the name of the SUBJECT in the lower part and the Date and number of the file in the right portion of the paper. EXAMPLE:

BENITEZ, Wilfredo D. DATE: 1 May 1988
FILE NUMBER: 50-88-0-1

H. Complete the "Distribution" Section in block #24. The distribution of the report will be made according to its SOP.

I. Complete the "Reviewed by" section in block #25. The typewritten name and signature of the authority that reviewed the report is written down in this section.

INVESTIGATION REPORT DATE SUBMITTED

FOCUS

(HISTORY) CASE CLASSIFICATION

_____RAL _____RAG _____IAE _____IAI

IDENTIFICATION DATA

1.LAST NAME FATH. MOTH. NAM., INIT. 2.I.D. 3.RACE 4.RANK 5.BRANCH

6.POSITION7.

DATE OF BIRTH 8. PLACE OF BIRTH

9. UNIT OR EMPLOYMENT ADDRESS 10. RESIDENTIAL ADDRESS

11. INCIDENT'S TITLE 12. INCIDENT'S DATE 13. INCIDENT'S TIME

14. LOCAL

(BUILD. UNIT) 15. EQUIPMENT, ETC. SERIAL NUM.

CONTROL DATA

16. CONTROL SYMBOL OR FILE NUMBER

17.

INVESTIGATION DONE BY (ORG.) 18. CONTROL OFFICE

INVESTIGATION DATA 19. INVESTIGATION REQUEST BY 20.

REASONS FOR INVESTIGATION

21. INVESTIGATION DATE
START COMPLETION

22. PRESENT CASE SITUATION

_____CLOSED _____FINISHED ______SUSPENDED ______PENDING

23. SYNOPSIS

24. DISTRIBUTION

25. REVIEWED BY
NAME AND TITLE SIGNATURE

CHAPTER XX

PREPARATION OF SUMMARY REPORTS

INTRODUCTION:

A summary report (SR) is the vehicle used to summarize certain aspects of an investigation, or give emphasis to key points of actions in an investigation. This report is not as detailed and is not designed to replace the Agent's Report. It is as the title implies, a summary. The (SR) must contain certain favorable or derogatory (unfavorable) concise information declarations, if it applies, this way the perspective of the case or investigation will not be altered.

GENERAL FACTS:

A. Preparing the heading.

1. Write down the preparation date in the "Date" section.

2. Write down the identity of the "Preparing Office".

3. Write down the SUBJECT'S information using the same rules in the Agent's Report.

a. Father and mother's last name in capital letters, name, initial.

b. Identification number.

c. Date and place of birth (FDLN).

EXAMPLE: PEREZ-RIVERA, Juan A.
I.D. NUMBER: 111-11-1101
PDOB: 1 January 1947, San Miguelito, ES

B. Write down the information to be reported in the "Summary Report" section. The text starts in the third line of the black line in the upper part of the block titled "Summary Report", leaving two lines in the upper part. The line or black border to the left of the document is used as a margin for all items.

1. Write down the numbers in sequence. For example:

1.

2.

3.

2. Write down the classification contained in each paragraph. For example:

1. (C)

2. (S)

3. (NC)

3. Write down the evaluation code (key word) of the information content of each paragraph using the evaluation system shown in the SR. The evaluation code must be written down in the last line of the paragraph in the right edge (Figure 1).

NOTE: If there is not enough space to write down the evaluation code in the last line of the paragraph, the evaluation code will be written down in a line below the last line of the paragraph and in the extreme right of the document.

Example:____

____

____

______he left in a Toyota with Cuban license plates.

(F-6)

C. Information Sources.

Information sources normally are not revealed in the SR. If the report is kept within military intelligence, the source could be identified if the identification is necessary to establish the truth of the information. When the source is not identified, for security purpose, an indication of the access to the information could be included while the information about the source is not as explicit that it identifies the source. When the SR does not reveal the source's identity the copy of the office files should write down the source(s) identity. A code number must be used when the source's identity requires protection. Bibliographies of the sources could be added in the files when using more than one source for the same report.

D. Information from other government agencies. Information obtained form other government agencies, except from the Armed Forces, will not be included in the SR. If other agencies outside the Armed Forces solicit the information obtained in the SR, the originator or the source must give permission for the information to be divulged. If the SR contains information that has been authorized to be divulged to other agencies, this information will be written in capital letters and underlined.

Example: THE SOURCE WHO IS CONSIDERED TRUSTWORTHY INFORMED THE ______________________________

__________(Figure 1, Paragraph 4).

When this type of information appears in the SR, the following declaration must be included and must appear as a non-numbered paragraph and at the end, written in capital letters. (Figure 1, Paragraph 4).

Example: INFORMATION FROM OTHER SOURCES OUTSIDE THE SOURCES FROM THE ARMED SOURCES ARE INCLUDED IN THIS SR. THIS INFORMATION WILL NOT BE DIVULGED TO ANY OTHER AGENCY OUTSIDE THE ARMED FORCES.

E. Additional space. If you need additional space, two lines in the lower part of the document will be left blank and the text will continue in blank paper witn normal margins. In the upper part of the white paper, the SUBJECT'S block will be placed at left with the date and reference files.

Example:
PEREZ-RIVERA, Juan A.
I.D. NUMBER: 111-11-1101
PDOB: 1 January 1947, San Miguelito, ES

1 August 86

he came into the restaurant and sat down at the corner table where was accompanied____

F. SR distribution. The last item of the SR is the distribution. The distribution will be indicated according to the SOP. (Example in figure 1).

G. Closing the SR. The SR is not signed. The file copy will have the person's name who prepared the SR typewritten in the upper part at the document's right corner.

H. The SR will be classified according to its content.

SUMMARY

REPORT DATE

PREPARING OFFICE

SUBJECT

SOURCE'S EVALUATION CODE ABOUT THE INFORMATION
COMPLETELY TRUSTWORTHY A CONFIRMED BY OTHER
NORMALLY TRUSTWORTHY B SOURCES 1
COMFORTABLY TRUSTWORTHY C PROBABLE TRUTH 2
NORMALLY NON-TRUSTWORTHY D POSSIBLE TRUTH 3
NON-TRUSTWORTHY E DOUBTFUL TRUTH 4
TRUST NOT KNOWN F IMPROBABLE 5
TRUTH CANNOT
BE JUDGED 6

SUMMARY REPORT

DISTRIBUTION

CHAPTER XXI

SCRUTINY OF CI INFORMATION

INTRODUCTION:

SCREENING

The scrutiny process and CI interrogation allows us to identify and explore the persons/targets of interest to CI. This process allows us to detect these persons or targets, it helps us in the imposition of the same in an effective manner.

GENERAL FACTS:

A. DETERMINE THE PURPOSE OF THE SCRUTINY AND CI INTERROGATION:

1. The CI scrutiny operations, submit, in a systematic way, the civilians in the combat area to a series of questioning/interviews/interrogations with the purpose of:

a. Find and segregate suspicious persons.

b. Identify persons of interest to the CI. (See Example #1).

NOTE: THE CI SCRUTINY OPERATIONS ARE CARRIED OUT TO INTERCEPT ENEMY INTELLIGENCE AGENTS, SABOTAGE AGAINST, INSURRECTION TRYING TO INFILTRATE OUR AREA OF OPERATIONS.

c. Obtain information of immediate value to the intelligence.

d. Obtain information that normally will not be available to the intelligence units.

2. The CI interrogation operations are carried out to obtain the maximum amount of information about the enemy's intelligence operations in the least possible time.

B. Determine the types of scrutiny operations necessary to satisfy search requirements and CI operations.

EXAMPLE #1

VARIED CATEGORIES OF PERSONS THAT ARE OF INTEREST TO CI

1. REFUGEES AND DISPLACED PERSONS

2. BORDER CROSSERS

3. ENEMY UNITS DESERTERS

INTERNEES

4. CIVILIAN PRISONERS AND WAR PRISONERS

5. CONCENTRATION CAMP CAPTIVES

6. RESISTANCE ORGANIZATIONS MEMBERS WHO ARE INTERESTED IN JOINING OUR LINES

7. ENEMY COLLABORATORS

8. CI TARGETS, SUCH AS THOSE APPEARING IN BLACK, GREY AND WHITE LISTS

9. VOLUNTARY INFORMANTS

10. PERSONS WHO HAVE TO BE INTERVIEWED BECAUSE THEY ARE UNDER CONSIDERATION FOR EMPLOYMENT WITH THE DEFENSE FORCES OR WITH THE CIVILIAN AFFAIRS OFFICE.

1. You must establish operations with a central scrutiny focus normally in the area of collection of war prisoners. This central scrutiny point:

a. Has as purpose to receive, segregate, investigate and classify war prisoners, border crossers, refugees, etc.

b. Receive persons captured by combat troops, support and logistics within the operations area.

2. Fixed checking points, are permanently occupied by combat troops or military police with the support of interrogation agents or CI personnel, in the entrance to towns, crossing of rivers, and in other similarly strategic areas.

3. Mobile checking points, (in vehicle, or on foot) are used as a mobile system for choosing persons of interest at random. This point must be located in various places and should not be fixed in the same place for longer than a day.

4. Cordon ~~Wall-in~~ and search operations are used to segregate the town, area or valley, investigate the inhabitants and search residences and public areas.

D. Determine the personnel requirements: The normal investigation equipment are Military Police, combat troops, civilian affairs personnel, interrogation agents and CI agents.

E. Determine the specific method of identifying persons of interest to CI:

1. Carry out initials interrogations of chosen civilian and military personnel.

2. Use the black, grey and white lists.

3. Use an informant/source who is infiltrated in prison cells or detention centers/war prisoners.

4. Place recording or sound equipment in the detention areas of refuges or war prisoners.

5. Distribute a list of CI indicators of interest among the military police, interrogation agents, civilian affairs personnel and any other personnel involved in investigations. (SEE EXAMPLE #2).

EXAMPLE #2

CI INDICATORS OF INTEREST

1. PERSONS IN MILITARY AGE
2. PERSONS WHO TRAVEL ALONE OR AS A COUPLE
3. PERSONS WITHOUT PERSONAL IDENTIFICATION
4. PERSONS WITH STRANGE DOCUMENTS
5. PERSONS WHO HAVE GREAT AMOUNTS OF MONEY, JEWELS IN THEIR POSSESSION.
6. PERSONS WHO SHOW UNUSUAL ACTIONS
7. PERSONS WHO TRY TO AVOID DETENTION OR INTERROGATION
8. PERSONS WHO USE ENEMY'S METHODS OF OPERATION
9. PERSONS KNOWN AS ENEMY SYMPATHIZERS
10. PERSONS WITH A SUSPICIOUS HISTORY BACKGROUND
11. PERSONS WITH RELATIVES IN THE ENEMY'S AREA
12. PERSONS WHO HAVE TECHNICAL SKILLS OR SPECIAL KNOWLEDGE
13. PERSONS WHO HAVE COLLABORATED
14. PERSONS WHO DISOBEY THE LAWS IN THE ENEMY'S AREA

E. Examine the files of the data base from the infrastructure of the enemy's intelligence so as to become familiar with:

1. Operation methods

2. Procedures/rules

3. Objectives

4. Offices and sub-offices

5. Known agents

F. Study the areas under the enemy's control so as to become familiar with:

1. The geography

2. Points/historical or tourist areas

3. Distances and road conditions

4. Political situation

5. Social and economic traditions

6. Traditions and customs

7. Racial problems

G. Analyze the operations area to determine:

1. Curfews

2. Movement restrictions

3. Rationing

4. Obligatory service for army

5. Labor civilian programs

6. Requisite to become a member in political organizations

7. Other restrictions that have been imposed by the population

8. Acquiring knowledge of all the restrictions that have been imposed to the population could help you to:

a. Detect discrepancies

b. Recognize changes in enemy activities

c. Maintain control

H. We must study the situation and the files of the order of battle to become familiar with:

1. Enemy units in the area of operations

2. Enemy units adjacent to area of operations

3. Dispositions

4. Capacities

5. Weaknesses/vulnerabilities

6. Composition

7. Training

8. Equipment

9. Activities or recent operations

10. History

11. Personalities and commanders

I. Analyze the intelligence priority requirements of the commander to recognize, detect, explore and report the facts of the Order of Battle (OB).

NOTE: THE CI AGENT DOES NOT QUESTION THE SUSPECTS WITH THE PURPOSE OF OBTAINING INFORMATION FROM OB; NEVERTHELESS, EACH CI AGENT MUST FAMILIARIZE HIMSELF WITH THE COMMANDER'S RPI/RI TO RECOGNIZE PERSONS WHO POSSIBLY HAVE THE OB INFORMATION.

J. Prepare a list of indicators to help the investigations personnel in identifying the hostile infiltrators/enemies.

L. Coordinate with:

1. The commander in regards to the segregation of refugees and war prisoners in your area of operation.

2. The military police for the control of evacuation of refugees and war prisoners.

3. With the G5 for the support of civilian affairs and psychological operations.

4. The civilian authorities if the control of the area has been returned to them.

5. With the interrogation agents to:

a. Agree on the categories of persons that will be transferred to CI control for further questioning.

b. Decide where to place the CI interrogation agents and the methods use to transfer the detained from one place to another.

M. To carry out the initial investigation of the persons:

1. You must segregate the detained, if they are more than one, according to the following manner:

a. Civilians from military men

b. Officers from troop soldiers

c. You must segregate them even more if necessary according to:

1. Nationality

2. Sex

3. Rank

4. Branch of military service

NOTE: YOU SHOULD SEGREGATE PERSONS IF THERE IS ENOUGH PERSONNEL AVAILABLE TO CARRY OUT THIS OPERATION.

2. Determine the apparent level of knowledge of the person evaluating the following:

a. His physical appearance.

b. All documents, arms and equipment held that was captured with the person.

3. Select personnel of CI interest, comparing the person with the indicators in Example #2 and the type of persons in Example #1.

N. Carry out the interrogations of specific persons

O. Make a disposition of the persons:

1. Exploit persons who have access and are settled in areas of interest.

2. Transfer these persons to the central point of investigation to be re-introduced to the flow/group of war prisoners and refugees.

P. Complete the required reports.

CHAPTER XXII

CI INTERROGATION OF SUSPECTS

INTRODUCTION:

special

The CI espionage agent in combat could only have a minimum amount of information with which to conduct the work or have minimum knowledge of the situation and the area. In spite of his conclusions been based in that minimum amount of information, he must be impartial in the search for facts. As a CI espionage agent
you must have two things in mind in working as an interrogator, the detection and prevention of a threat and the security of the armed forces and the collection of information of interest for the departments of intelligence.

GENERAL FACTS:

A. Carry out an exhaustive study of all the material available in the case under investigation:

1. The interrogation is the art of questioning and examining a source to obtain the maximum quantity of useful information. The goat of interrogation is to obtain true and useful information in a legal manner and in the minimum amount of time possible.

2. To do effective work and carry out a logical sequence of questions, you must always have in mind all that you know to that moment about the case under investigation.

a. Identify yourself to all persons involved in the incident, including witnesses, victims, and investigations.

b. Identify the exact circumstances of the incident occurred.

c. Determine where each incident happened or activity.

d. Identify how it happened.

e. Identify why it happened.

2. Pay particular attention to all the details of the case, especially those details that are not of public knowledge as yet.

d. Become familiar with the legal aspects and procedures that apply to the case.

a. Identify the elements of the crime that could help you determine the objectives of the interrogation.

b. Identify the ilegal or prohibited methods. Do not use force, mental torture, threats, insults or exposition to cruel or inhuman treatment of any sort.

NOTE: IN CASE THAT THERE IS DOUBT IN REGARDS TO THE LEGALITY OF A METHOD, CONSULT WITH AN AUTHORITY IN A HIGHER ECHELON TO CLARIFY THE DOUBTS.

B. Identify possible suspects for interrogation:

1. Become familiar completely with the history of the suspects. History data of particular interest during the interrogation include:

a. Age, place of birth, nationality and race.

b. Rank, or position in the community.

c. Level of education.

d. Present and past occupations.

e. Habits.

f. Associates (business partners)

g. Criminal history.

NOTE: IF IT IS POSSIBLE TO OBTAIN THIS INFORMATION BEFORE THE INTERROGATION, OBTAIN IT FROM THE SUSPECT DURING THE INITIAL PHASE OF THE INTERROGATION.

3. Use the history of the suspect information to:

a. Develop the best method of questioning

b. Prove the truthful intention of the suspect

c. Impress the fact to the suspect that the detailed fact is the investigation of the case.

3. Determine the available information, what type of attitude is expected from the suspect.

a. Cooperative and friendly: Offers little resistance and he will talk freely about almost any theme.

b. Neutral and non-sharing: Will cooperate up to a certain point. Direct questions and to the grain of the matter will have to be used to obtain the answers.

c. Hostile and antagonistic: Frequently, will refuse to talk and will offer much resistance.

4. Classify the suspects according to the following:

a. Persons with previous offenses and whose guilt is almost certain according to information already available.

b. Persons whose guilt is doubtful or uncertain due to the weak evidence available or the lack of essential facts.

5. If possible, carry out a visual observation of the suspect before the interrogation takes place to identify weaknesses that could be exploited during the interrogation.

C. Prepare an interrogation plan:

1. Identify the objective of the interrogation:

All interrogation must have a defined purpose. This purpose must be kept in mind during the entire preparation process and when the interrogation is carried out. But, it must not be concentrated so much in the objective as to allow another valuable information.to be overlooked during the interrogation.

2. Identify the type of interrogation:

a. Direct interrogation: The suspect knows that he is been interrogated. Nevertheless perhaps he does not know the true objective of the interrogation. This method takes less time than the other one.

b. Indirect interrogation: Obtain information through deception. The suspect does not have any idea that he is been interrogated. This method requires a careful planning, extreme discretion, and must be applied with much skill.

3. Identify and obtain the helpful things required for interrogation:

a. Files

b. Documents

c. Maps/charts

d. Pencil, notebooks, tape recorder, etc.

e. Any other equipment that could facilitate the process of interrogation.

4. Identify the approximation methods that will be used during the interrogation:

NOTE: SELECTING AN INITIAL APPROXIMATION IS NECESSARY, BUT YOU MUST KEEP THE FLEXIBILITY OF MOVING FROM ONE APPROXIMATION METHOD TO ANOTHER.

5. APPROXIMATION METHODS:

a. DIRECT APPROXIMATION: Do not try to hide the purpose of the interrogation. It works better when it is used with persons whose guilt is almost certain and with those persons that have little knowledge of what security is. It is a good method to interrogate persons of low level or rank in organizations. This method takes little time and is simple. This method offers the best opportunity to demonstrate empathy and understanding to the suspect. Act as if the offense is something that the suspect will not commonly do. Treat the suspect as a rational person who was only exposed to the circumstances of the case.

b. FILE AND DOSSIER: Prepare a file that contains all the information collected about the suspect. A careful arrangement of the information in the file could give the appearance of having much more information than it really has. Put additional papers, although they do not contain information to just give the appearance of an enormous file. Mark the file with different sections/areas of interest about the history of the suspect. Confront the suspect with the file and warn him that it contains detailed information of his background history and activities and that it is useless for him to refuse to cooperate in the interrogation. The triumph of this method depends upon the immaturity of the suspect, the amount of information available, and the skills used by the interrogation agent to convince the suspect.

c. WE KNOW IT ALL: Make questions based upon information that is already known to us. When the suspect refuses to answer, hesitates, or provides incorrect information, you yourself provide the information or correct answer. If it is used correctly, you may convince the suspect that we know it all and that his answers are not of real importance. When the suspect starts to answer truthfully, weave other questions, of which we do not have the answers. Always verify the truthfulness of the suspect starting to make the questions of which we know the information. This method could be used with or without the files and dossier method.

d. FUTILITY/USELESSNESS: You must convince the suspect that resisting to answer to the interrogation is useless. Present true information to the suspect in a persuasive and logical manner to exploit the psychological and moral weaknesses of the persons.

e. QUICK SHOT: Make a series of questions to the suspect in a way that he will not have time to answer one before the next one is made. Since the suspect does not have time to formulate his answers he will get confused and could contradict himself. Confront him with the inconsistence of his answers, so that perhaps he may reveal more information than he wishes. This provides leads to further questions. Prepare all questions beforehand. Use a competent experienced interrogator. Use this method immediately after his arrest to take advantage of his state of confusion.

f. INCENTIVE: To reward the suspect's cooperation and the fact of telling the truth, this is attained normally by providing him with some physical commodity, (cigarettes, sweet, coffee, etc.) that normally is not given to him. Do not make promises or commitments that are beyond your ability to fulfill. Use caution to avoid that the suspect gives false information with the intention of getting the article he wishes. Never deny the basic articles of human needs. Do not use the threat of taking food so as to obtain his cooperation.

g. REPETITION: Make a question, wait for the answer, and repeat the question and the answer several times. This is done with all questions until the suspect is totally bored and starts to give unexpected answers so as to break the boredom. This method works better with a hostile person. Generally it does not work with an introverted or timid person.

h. MATT AND JEFF: You must use two experienced interrogators that could develop two different personalities towards the suspect. The first interrogator acts very formal, little sympathetic, and at times rude, noisy and aroused. The second interrogator appears when the suspect feels lost and alone. The second scolds the first interrogator for his poor professional conduct and orders that he leaves the interrogation room. The second interrogator apologizes with the suspect and tries to calm him. He shows empathy with the suspect and tries to establish some common ground between the two, for example: both are intelligent and sensitive, while the first interrogator was not. The idea is that the first interrogator could return to the interrogation and help if the suspect stops to cooperate.

very bad word.

i. PRIDE: This method could be used in two ways. Attack the pride of the suspect accusing him of being weak or insinuating his poor ability to do anything. The suspect who is proud will hurry to defend his abilities. Frequently this will explain why he did or did not do something just to defend his honor. You may obtain important information from his answers. The other way to use this method is to praise the suspect until you get him to admit certain information as a way of reclaiming responsibility/credit. This brings the suspect an opportunity to boast what the has done.

j. SILENCE METHOD: Do not say anything to the suspect, but look at him fixedly in the eyes. Do not move your gaze, but make him break the eye contact. As the suspect gets nervous, he will start to make questions, but do not break the silence until you are prepared to do so. Keep this method for some time and the suspect will get nervous. When breaking the silence you must question the suspect with questions that indicate his guilt.

k. CHANGE IN SCENARIO: Take the suspect out of the interrogation room environment. Take the suspect to a more peaceful but controlled area that could give the opportunity to have a peaceful and nice conversation during which you may pull the necessary information from the suspect.

l. ESTABLISH HIS IDENTITY: It is alleged that the suspect is not the person he claims to be, but that he is a person who the police authorities are searching for political assassinations and acts of terrorism and treason, or any serious accusation. In his intent to establish his identity, the suspect could give valuable information and leads for further investigations.

m. EMOTIONAL: Determine what emotion motivates the suspect (hate, love, vengeance, desire to make money) and exploit that emotion. This method is very effective when you use immature and timid persons.

5. Develop detailed questions to use during the interrogation:

a. Develop questions that guarantee that the area of interest is exploited.

b. Develop questions that establish all facts (who, what, when, where, why and how).

c. Develop control questions of which the answers are already known.

d. Develop non-pertinent questions if the true objective of the interrogation is been hidden from the suspect. Use non-pertinent questions to break the suspect's concentration.

e. Develop repeated questions making the same questions but in a different way.

f. Develop direct questions that require a narrative answer.

g. Develop follow-up questions that allow the expansion of themes/areas as they become necessary.

D. Select the interrogation personnel based in the selected approximation, type of suspect, and the ability of the interrogation agents.

1. Select an interrogation agent that has personality characteristics that are adequate and an interest in human nature. Personal qualities desired in an interrogation agent are:

1) Motivation

2) Be alert

3) Patience and tact

4) Objectivity

5) Credibility

6) Adaptability

7) Perseverance

8) Linguistic skills

2. Select an interrogation group, if possible. It is necessary to have a group to successfully use much of the approximation methods already discussed. Additionally, an interrogation agent could notice that he cannot obtain the necessary information after having used various approximations and techniques, or is tired in the middle of a long interrogation. This could cause the loss of control of the interrogation and another interrogation agent must replace the first.

E. Guide the interrogation group in the approximation methods already selected and the role that each one will play in the interrogation.

F. Make all the arrangements in regards to the suspect:

1. Coordinate the arrest of the suspect.

a. Make arrangements with the police to detain the suspect.

2. Make the arrangements to locate the suspect and give him board after the arrest.

3. Coordinate the use of facilities to give food to the suspect.

4. Coordinate the services of an interpreter if necessary.

5. If the suspect is of the opposite sex coordinate the presence of a witness of the same sex if necessary. It is also good to coordinate the presence of a witness to observe how the information is obtained; and so as to avoid that the suspect accuses us of using ilegal tactics such as torture, coercion and mental abuse.

a. Obtain the authorization of the commander to use a witness in the interrogation.

NOTE: IF THE SUSPECT IS OF THE OPPOSITE SEX, INFORM HIM OR HER OF HIS OR HER RIGHT TO HAVE A WITNESS OF THE SAME SEX PRESENT DURING THE INTERROGATION. IF THE SUSPECT DOES NOT WISH TO HAVE A WITNESS OF THE SAME SEX PRESENT, OBTAIN A SIGNED SWORN DECLARATION, INDICATING THIS WISH. (ALTHOUGH THE SUSPECT REFUSES TO USE A WITNESS, PLACE A WITNESS OF THE SAME SEX AT A DISTANCE THAT COULD LISTEN TO WHAT GOES ON DURING THE INTERROGATION WITHOUT BEEN SEEN BY THE SUSPECT.

G. Select and prepare the interrogation room:

1. Select a room that gives privacy during the interrogation. Eliminate all distraction possible.

2. Select a room that allows you to control the physical environment.

3. Select a room that has a nice constant temperature.

4. Arrange the furniture in the interrogation room. The furniture must be only a small table to write, but that does not give an area in which the suspect could hide under, and three chairs.

5. Place all material necessary during the interrogation in the room. Materials such as paper, pencil, reference manuals and other interrogation aids.

NOTE: DO NOT HAVE A TELEPHONE OR ANY ARTICLE THAT COULD BE USED AS AN ARM IN THE INTERROGATION ROOM.

H. Install and test the recording equipment. Use the recording equipment so that you could keep your concentration during the interrogation. Taking notes during the interrogation could break the rhythm of the questioning and it could cause you to loose the sequence of the questions and the concentration.

1. Install the recording equipment so that it is looks as if it is part of the furniture of the office.

NOTE: TO USE THE RECORDING EQUIPMENT, FIRST CONSULT WITH THE SUSPECT AND GET HIS PERMISSION.

2. Test the equipment to make sure that it is functioning correctly.

I. Receive and identify the suspect:

1. During the initial contact keep a professional posture and try to gain the trust of the suspect.

2. Verify the identity of the suspect and examine his personal documents.

J. Identify yourself and the other members of the interrogation equipment. Use your official badge to make sure that the suspect knows your identity as a member of the military intelligence.

K. Explain to the suspect that the nature of the accusation is against his behalf.

[page missing]

b. Try to identify contradictions and weaknesses in the history of the suspect.

5. Change interrogation agents if the first interrogation agent cannot obtain true information or a confession after having used various approximation techniques.

6. If all the approximations fail with the suspect, confront him with crime witnesses if possible.

7. If necessary, make a final convincing appeal against the suspect's continuous resistance.

a. Insist in appealing the existence of all evidence against him.

b. Confront the suspect with the contradictions and weaknesses in his history.

Q. If the suspect admits culpability, obtain a sworn declaration signed by him.

R. CLOSING PHASE OF THE INTERROGATION:

1. Close the interrogation for any of the following reasons:

a. If the suspect is sick, wounded, or advanced age and needs medical attention.

b. Various interrogations are necessary to obtain all the necessary information.

c. The suspect is bored and denies to cooperate.

d. All the questions have been answered and the requirements of the interrogation have been satisfied.

e. The initiative has been lost and you as interrogation agent decide to close the interrogation.

2. When the interrogation is closed, always consider the possibility of interrogating the suspect again.

a. Finish the interrogation in a nice manner.

b. Re-emphasize the approximations used to gain confidence from the suspect.

c. Give opportunity to the suspect to add additional information to the one already given.

3. Use the time dedicated to the Closing to try to obtain information that may have not been discussed during the interrogation. A suspect could relax a little more after knowing that the interrogation has been finished and he could reveal additional information.

S. Disposing of the suspect:

1. Have the police put him under custody.

2. Give the suspect to pertinent civil authorities.

3. Give the suspect to the commander's custody.

T. PREPARE THE REQUIRED REPORTS

CHAPTER XXIII

EXTRACTING CI INFORMATION

INTRODUCTION:

Wheedling is applied always with a specific purpose in mind. The objective, or the information desired, is the SUBJECT'S determining factor, of the wheedler, and the environment.

GENERAL FACTS:

The word is Elicitiation

A. Definition of ~~WHEEDLING~~: Wheedling is the technique of obtaining the greatest amount of information/useful intelligence, from a person or source, so that the person does not know our purpose.

1. Before starting the wheedling there are requirements of CI collection to be reviewed:

a. Identify the required specific information.

b. Identify the wheedling objective.

2. Select the SUBJECT of the wheedling according to his access to, or knowledge of, the information desired.

3. Obtain and evaluate all information available in regards to the SUBJECT in the wheedling:

a. Carry out the review of files and try to obtain the following information about the SUBJECT:

1) History

2) Motivations

3) Emotions

4) Psychological nature

5) Habits or patterns

6) Favorite visiting places. (bars, restaurants, discos, etc.)

7) Favorite hobbies

8) What level of knowledge he has about security that person has.

9) If he has been previously used in other wheedling intents by other CI agents.

4. Determine in what place/specific environment the wheedling will take place.

a. Select the place where the approximation to the SUBJECT/Source will take place.

NOTE: A SUBJECT must be approached in a natural environment to avoid raising his suspicion.

b. Obtain al the information about the place selected:

1) Identify all the place's irregular traces or facts.

2) Identify what type of clothes will be required to enter that place. (Formal: shirt and tie; Informal: shorts, jeans, etc).

3) Identify the money requirements. (It is a place where food or products are expensive or cheap).

4) Identify possible security problems

5) Identify if the place has been used previously as a wheedling place.

c. Select the date and time more desirable for the approximation.

5. Select for yourself a logical story (cover), one that could be credible and is according with the situation. The history must explain:

a. The reason you have to be in the chosen place for the approximation.

b. The agent's actions during the conversation.

6. Carry out the approximation using one of two approximation techniques: Flattery and Provocation, or any variation of these two techniques as mentioned below:

a. Use the flattery method:

1) Appeal to the ego, pride of the SUBJECT. Give him (SUBJECT) the opportunity to show pride or so that he flatters himself about his triumphs and gains.

2) Insinuate that the SUBJECT is an expert in a specific area, topic or theme. In this manner you will give him the opportunity to feel as if he is the teacher and you are the pupil.

3) Offer him (SUBJECT) valid and honest assistance.

4) Discuss areas of mutual interest. (Hobbies, work, sports, etc.)

NOTE: The agent must have a good knowledge of the theme he thinks he will choose to show mutual interest (that is to be able to follow the conversation professionally).

b. Use the approach method of provocation to open the conversation with the SUBJECT:

1) Adopt an attitude as if you do not believe what the SUBJECT says:

"What you say, is very difficult to believe, you have to explain it to me in more detail to see if it is true".

2) Insinuate that the SUBJECT really does not know anything of what he is talking about.

7. Once the approach has taken place, take the conversation to the area of interest:

a. Try to obtain more information give him answers that the SUBJECT finds obscure and that require more information to clarify them.

b. Ask the SUBJECT for more. information when his answers are not clear enough: ("I agree with you, although, what does it mean....").

NOTE: Be persistent without being abusive, bored or insolent.

c. Present a hypothetical situation that could be associated with an idea or thought expressed by the SUBJECT.

NOTE: Many persons that normally do not make comments about a real situation, will give his opinion about hypothetical situations.

d. Use your imagination and initiative to keep complete control of the conversation at all times.

8. Finish the [unclear] a. Use the flattery method:

1) Appeal to the ego, pride of the SUBJECT. Give him (SUBJECT) the opportunity to show pride or so that he flatters himself about his triumphs and gains.

2) Insinuate that the SUBJECT is an expert in a specific area, topic or theme. In this manner you will give him the opportunity to feel as if he is the teacher and you are the pupil.

3) Offer him (SUBJECT) valid and honest assistance.

4) Discuss areas of mutual interest. (Hobbies, work, sports, etc.)

NOTE: The agent must have a good knowledge of the theme he thinks he will choose to show mutual interest (that is to be able to follow the conversation professionally).

b. Use the approach method of provocation to open the conversation with the SUBJECT:

1) Adopt an attitude as if you do not believe what the SUBJECT says:

"What you say, is very difficult to believe, you have to explain it to me in more detail to see if it is true".

2) Insinuate that the SUBJECT really does not know anything of what he is talking about.

7. Once the approach has taken place, take the conversation to the area of interest:

a. Try to obtain more information give him answers that the SUBJECT finds obscure and that require more information to clarify them.

b. Ask the SUBJECT for more information when his answers are not clear enough: ("I agree with you, although, what does it mean....").

NOTE: Be persistent without being abusive, bored or insolent.

c. Present a hypothetical situation that could be associated with an idea or thought expressed by the SUBJECT.

NOTE: Many persons that normally do not make comments about a real situation, will give his opinion about hypothetical situations.

d. Use your imagination and initiative to keep complete control of the conversation at all times.

8. Finish the wheedling as soon as you obtain all the information desired:

a. Change the conversation theme to others before leaving and bidding goodbye to the SUBJECT.

b. Present various non-pertinent themes to avoid that the SUBJECT discovers its true purpose. (Wheedle intelligence information).

c. Finish the conversation in a normal manner.

9. Take notes of all the official funds expenses.

B. Prepare the required reports.

CHAPTER XXIV

DETECTING CI TARGETS

INTRODUCTION:

The identification of CI targets are done through the intelligence rules. A data base with a line and block box, used in connection with existing black, grey and white lists, intelligence reports and additional information from the police agencies, army and other agencies, provides us with basic information required to identify the potential CI targets.

GENERAL FACTS:

A. Review the CI estimate to determine the hostile threat:

1. Identify those threats to security that are of an immediate nature.

2. Identify anticipated future threats.

NOTE: The selection of CI targets must be based in an evaluation of a complete hostile threat.

B. Identify the specific CI targets of the local area:

a. The CI targets are of interest due to the threat that they present, or the usefulness to the Armed Forces. CI targets include:

a. PERSONALITIES (SEE FIGURES #2, 3 and 4): that could or not be friendly or hostile.

b. INSTALLATIONS (SEE FIGURE #5): that represent a threat to the national security.

c. ORGANIZATIONS AND TeamS (SEE FIGURE #6): that represent a threat to the national security. Its threat perhaps is not openly detectable due to their undercover operation methods.

d. DOCUMENTS AND MATERIALS (SEE FIGURE #7): with value to the intelligence or the counter intelligence.

NOTE: Use the CI Work Sheet (SEE FIGURE #1) as the principal paper to assist in the development of the targets:

3. Obtain information about the potential CI targets in the local area:

a. Extract the local targets from the CI target lists at national level.

b. Extract information from the existing Black lists (SEE FIGURE #2), White (SEE FIGURE #3), and Grey (SEE FIGURE #4).

c. Extract information from the intelligence files, CI data base, and similar files.

d. Obtain information from:

1) Civilian Affairs and Psychological Operations (G5)

2) Local intelligence units

3) Police elements

C. Categorize the CI targets identified by the specialty or function. Examples:

1) Espionage agents
2) Sabotage specialists
3) Messengers
4) Camps or bases
5) Communications and link routes

NOTE: To categorize the targets in this manner, it is essential that the history detailed information is obtained from the same source that was used to identify them.

D. Assign priorities to the targets:

1. Determine the priority of each Target based on:

a. The threat to the national security that the target represents.

b. The urgency or the need to neutralize or exploit the target.

c. The future capacities that await the target.

d. The capacities of the units responsible to neutralize or exploit the targets.

2. Assign a numerical priority to each target:

a. The numerical designations are always expressed in roman numerals (I, IV, XI).

b. The numerical designation emphasizes the relative importance or the value of the CI targets.

c. The numerical designation expresses the level of interest of the target.

NOTE: If a target has been assigned a priority at a level higher than the Command, you at your level cannot alter this priority designation. The local CI elements will assign priorities to targets locally developed.

E. Assign the responsibilities of the units to neutralization or exploitation of each target:

1. Determine the capacities of the units to carry out neutralization or exploitation missions based on:

a. Amount of personnel
b. Equipment available
c. Specific experience

2. Identify the need, if any, to request support from the military police, infantry, national police, etc.

NOTE: The tactical effort, except in special cases, takes precedence over the neutralization and exploitation of the targets.

F. Notify the units of their mission(s).

FIGURE #1
CI TARGETS WORK SHEET

REFERENCES TO CHARTS, MAPS DATE:

KEYS TO CHART:

1. Target
2. Target classification
3. Priority
4. Localization
5. Team task
6. Team mission (Comments)
7. An administrative number that is written down in chronological order.
8. The classification identifies the target by type, name and provides specific data for identification about the target.
9. The priority is designated with roman numerals and is assigned based upon the target classification.
10. The localization will identify the place where you may find the target or if this is not known, it is identified where the target was found the last time.
11. The team's task of identifying the CI team whose mission is to neutralize the target is based in the number of persons available and could include tactical forces, military police and para-military forces.
12. This column is used to make a list of the coordination requirements, communications, specific details of the mission or other specific information required so that the team could fulfill its mission.

FIGURE #2
CI Target ~~BLAC~~K LISTS

THESE CONTAIN THE IDENTITIES AND LOCALIZATIONS OF PERSONS WHOSE CAPTURE AND DETENTION ARE OF FOREMOST IMPORTANCE TO THE ARMED FORCES:

EXAMPLES

a. Enemy agents known or suspects, persons involved in espionage, sabotage, politics, and subversive persons.

b. Hostile para-military guerilla team leaders, known or suspects.

c. Political leaders known or suspected as hostile toward the Armed Forces or the political interests of the National Government.

d. Known or suspected leaders of enemy governments whose presence in the area of operations represent a threat the national security.

e. Collaborators and sympathizers of the enemy, known or suspects whose presence in the area of operations represent a threat to the national security.

f. Military and civilian enemies, known or suspected of having participated in intelligence activities, counter-intelligence, security, police or political indoctrination between the troops or among civilians.

g. Other personalities identified by the G2 as of immediate detention. This could include local political personalities, chiefs of police, and municipal leaders or leaders of the enemy's government departments.

FIGURE #3
~~GREY LISTS~~ CI Sources

CONTAINS THE IDENTITIES AND LOCALIZATION OF THOSE PERSONALITIES WHOSE INCLINATIONS AND ACTIVITIES TOWARD THE POLITICAL AND MILITARY OBJECTIVES OF THE GOVERNMENT ARE OBSCURE (THAT IS, NOTHING IS KNOWN ABOUT THEM). THEIR INCLINATIONS OR ATTITUDES DOES NOT MATTER, IF THEY HAVE SOME INFORMATION OR SKILLS THAT ARE OF INTEREST TO THE NATIONAL GOVERNMENT. THOSE PERSONS WHOSE INCLINATIONS OR POLITICAL MOTIVATIONS REQUIRE MORE EXPLORATION OR EVALUATION BEFORE THEY COULD BE USED EFFECTIVELY BY THE GOVERNMENT CANNOT BE INCLUDED.

EXAMPLES

a. Defectors or potential defectors of the enemy cause whose motivation or loyalty has not been yet established.

b. Persons that have resisted or are believed to have resisted the enemy government and that perhaps are willing to cooperate with the Armed Forces of the National Government, but their motivation or loyalty has not yet been established.

c. Nuclear scientists, physicists and technical personnel suspected of having participated in development of nuclear projects for the enemy, or nuclear missile programs, against their will.

FIGURE #4
C i sources ~~WHITE LIST~~S

CONTAIN THE IDENTITIES AND LOCALIZATION OF PERSONS IN AREAS CONTROLLED BY THE ENEMY WHO HAVE BEEN IDENTIFIED AS OF INTEREST TO THE INTELLIGENCE OR TO THE COUNTER INTELLIGENCE, AND IT IS EXPECTED THAT THEY COULD PROVIDE INFORMATION OR ASSISTANCE IN THE ACCUMULATION OF INTELLIGENCE OR IN THE EXPLOITATION OF AREAS OF INTEREST. NORMALLY THESE PERSONS AGREE WITH, OR FAVORABLY BEND TOWARDS THE BELIEFS OF THE NATIONAL GOVERNMENT. THEIR CONTRIBUTIONS ARE BASED IN A VOLUNTARY AND COOPERATIVE ATTITUDE. THE DECISION TO PLACE A PERSON IN A WHITE LIST COULD BE AFFECTED BY THE COMBAT SITUATION, THE CRITICAL NEED FOR SPECIALISTS IN THE SCIENTIFIC FIELDS AND OTHER INTELLIGENCE`NEEDS.

a. Ex-political leaders of a hostile government that were deposed by the hostile political leaders.

b. Intelligence agents employed by the National Government.

c. Key civilians in the scientific development areas could include members of university faculties, whose loyalty has been established.

d. Religious team leaders and other humanitarian team leaders.

e. Other persons who could give significant material support to political objectives, scientists and military personnel of the National Government and whose loyalty has been established.

FIGURE #5
INSTALLATIONS

1. COMMAND POSTS.

2. COMMUNICATION CENTERS.

3. INVESTIGATION AND DEVELOPMENT CENTERS, LABORATORIES.

4. INSTALLATIONS THAT FORMERLY OR AT PRESENT ARE OCCUPIED BY ENEMY ESPIONAGE AGENCIES, SABOTAGE, AND INSURRECTION, OR ENEMY POLICE ORGANIZATIONS INCLUDING PRISONS.

5. INSTALLATIONS OCCUPIED BY ENEMY INTELLIGENCE ORGANIZATIONS OR SECURITY.

6. BELLIGERENT DEPOTS.

7. EMBASSIES OR HOSTILE GOVERNMENT CONSULATES.

8. MILITARY INSTALLATIONS.

9. PARA-MILITARY Team CAMPS

FIGURE #6
ORGANIZATIONS AND TeamS

1. Local or national political party teams, or parties that have goals, beliefs or ideologies contrary or in opposition to the National Government.

2. Para-military organizations including student teams, police, military and veterans, or ex-fighter teams that are hostile towards the National Government.

3. Teams or hostile organizations whose objective is to create dissention or cause restlessness among the civilian population in the area of operations.

4. The central offices of these hostile organizations according to what the Commander of the Armed Forces says will be immediately neutralized. Personalities related with these offices will be arrested and detained.

5. Teams that operate undercover or clandestinely and their infrastructure.

6. Intelligence networks.

FIGURE #7
DOCUMENTS AND MATERIALS

1. Files at bases, training centers and enemy intelligence schools.

2. Court files (Judicial), prisons, police, and the political administrative executives.

3. National intelligence agencies' files, para-military organizations, and the enemy's secret police agencies.

4. Products or other materials that, if left unguarded could provide support to the enemy guerrilla in the area.

5. Special war materials:

a. Chemical war products

b. Harmful materials

c. New combat products

d. Rockets and rocket control centers

e. Airships

f. Charts and maps warehouses

g. Communication equipment, including radios, radars and electronic equipment.

CHAPTER XXV]
NEUTRALIZING CI TARGETS

INTRODUCTION:

When identifying the potential CI target, those are categorized by their corresponding types. It is imperative to know not only the identity of the target or the team, but also all the possible history information and functions of the target. Experiences have shown us that a follow-up of a specific target, the best methods are traps and intercept tactics.

GENERAL FACTS:

A. Determine what Target is going to be neutralized.

B. Analyze the CI target work sheet (SEE FIGURE #1) to be able to identify:

1. The target that has been assigned to your CI team (columns 2 and 5)

2. The target localization (column 4).

3. The necessary requirements for this coordination (column 6).

C. Determine the method for neutralization of personalities:

1. Select the method to neutralize personalities:

a. Place the identity of the target in the black, grey and white lists (REFER TO CHAPTER XXIII).

NOTE: Placing the target identity in the above-mentioned lists do not neutralizes him if the target is "undercover" or "clandestine", but it constitutes the first phase of this type of neutralization and allows the friendly forces to detain the target if they find him in the area of operations.

b. Carry out the investigation operations and or approach and search and review to segregate, identify and detain the target personalities.

[REFER TO CHAPTER XXIV, DETECTING CI TARGETS, FIGURE #1--CI TARGET WORK SHEET)

c. Carry out the psychological operations against the personalities:

1) Carry out the propaganda operations to discredit the target.

NOTE: Operations of this type must be prepared in detail and coordinated through the G5 (Civil~~ian~~ Affairs).

2) Carry out operations so as to make the target supervisors loose trust in him.

3) Carry out operations so that the enemy believes that his agent(s) has been uncovered or committed.

d. Carry out Deceit/conceal operations. Neutralization through deception could work with the use of false information to confuse the target.

e. Neutralize the personality target through the capture, detention or the exile.

f. Use the population control and other resources:

1) Use controls to locate and capture the target, such as:

a) Search all persons in the target's area.

b) Give identity badges to the population.

c) Impose rationing of resources, such as, provisions, the food, etc., and give the population rationing cards.

NOTE: The targets that are of CI interest will try to avoid all these controls so as to avoid been captured or identified. Persons that do not have the badge in their possession or the rationing card, automatically will become suspicious.

2) Use controls to limit or slow down the movements of the target, such as:

a) Requiring official passes to access specific areas.

b) Implement a curfew which will restrict all movement during specific hours of the day.

c) Use restricted areas to deny the target to have access to certain activities.

2. Select methods to neutralize the teams. The same methods that are used to neutralize the personalities could be used for the teams. An additional method is to infiltrate an agent within the infrastructure of a team to spread rumors and false information.

3. Select a method to neutralize the installations:

a. Carry out approach, search and review operations to:

1) Segregate and contain the persons or teams in the particular installation or area.

2) Investigation, identification, and detention of a CI target.

b. Carry out combat operations to:

1) Segregate and contain the installations.

2) Detain the occupants.

3) Destroy the installation.

c. Carry out deception and conceal operations that cause the CI target to change the direction of his intelligence collection and to prevent him to concentrate with his main mission.

3) Select methods to neutralize documents:

a. The two basic methods to neutralize documents are:

1) Capture
2) Destruction

b. Any of the two methods could be carried out using the operations of review, investigation and combat mentioned above to effectively neutralize the documents and so prevent the enemy from using them.

D. Determine the operational requirements:

1. Determine the personal requirements (How many persons you need for the operation):

a. Determine the number of persons

b. Determine what qualifications and skills will be needed to fulfill the mission (interrogation agents, interpreters, etc.)

c. Determine what special support you need for the mission:

1) Support from the combat troops to close the area where the search and review operations will take place.

2) Military police to give support during the review operations.

3) Determine (if possible) if the installation area is mined or if it has traps (booby traps).

4) Determine what other additional support you may need.

2. Determine the team requirements:

a. Identify the arms that the teams will need to carry out the review and detention.

b. Identify what type of communications you will use.

c. Determine if you will need any codes or special key words.

d. Identify what transport support you will need.

e. Identify how you will transport the targets, or how you will evacuate the area.

3. Determine the time frame:

a. Determine how much time you will need to carry out the neutralization.

b. Identify the ideal time to carry out the attack against the target.

c. Determine if vigilance is needed and if there is enough time to carry out the same.

d. Determine on what date should the mission be completed.

E. Prepare the operational plan:

1. Coordinate with the appropriate commanders to get the support personnel.

2. Arrange the procurement of the specialized team.

3. Procure the official funds for the operation.

4. Procure the communication equipment.

5. Coordinate with the combat commanders in the area the whereabouts of the target.

a. Inform the commander when, where, what and how the operation will take place to avoid conflicts in your responsibility area.

b. Make arrangements for any assistance you may need while in that area.

c. Coordinate the support of (short and long arms) in case it would be necessary.

6. Guide the team over the concept of the operation. Make sure that all the members of the team are aware of their responsibilities.

7. Guide the support troops:

a. Explain in detail the role they will play in the operation.

b. Indicate if they need arms or specialized equipment.

c. Emphasize the need to fulfill the time frame requirements.

F. Carry out the operation:

1. Move towards the target.

a. Carry out a final check to make sure that all the participants understand their responsibilities.

b. Carry out a final coordination if necessary.

1. Safeguard the target:

a. Make sure that the troops are in their assigned positions.

b. Carry out the review and detention.

2. Dispose of the target:

a. Arrange the transfer of the target personnel and or the documents.

b. Destroy the target installations.

CHAPTER XXVI

OBSERVATION AND DESCRIPTION

INTRODUCTION:

Our ability to perceive depends upon our innate ability, experience and the training in regards to our surroundings and the environment. You must keep in mind that the word perceive means to see and understand.

GENERAL FACTS:

a. Definition: OBSERVATION: Is the ability to recognize what is happening around us and the environment. This is attained through the maximum use of the five senses. Carrying out a detailed observation allows a person to remember any object, or situation in a complete, clear and exact manner.

b. Observation requires a mental effort to identify, analyze and relate what is happening in our surroundings and the environment.

c. It is a normal thing that a person perceives or understands only that which interests him or what does not require much effort. Example:

(1) Women, in general, are more interested in colors, since their physical appearance depends on the exact combination of colors, therefore, a woman may have more knowledge in describing something she saw even ~~, although, only~~ for only a few seconds. She knows the different colors better and could bring an exact description of what she saw.

(2) In contrast, men normally do not know colors well, or do not pay much attention when they observe them. Men normally remember the basic colors. If a man observes an automobile involved in an incident and wishes to describe it he will probably say "it was a blue automobile", but if a woman makes the same description about the same automobile, maybe she will do it in this manner: "it was a light blue automobile, with black and white trims". This does not mean that all mean and women are the same, but it is something that happens often and could be considered as a patter in regards to observation.

d. To train in observing with exactness the CI Special Agent (SA) must:

(1) Practice continually and in detail to recognize what happens in his surroundings and environment and in that manner try to observe and understand the personalities, situations, objects and incidents.

(2) Replace the casual observations wit the studies and detailed observations.

(3) Train yourself and practice estimating:

a. The time (hours)
b. The speed of an object that is moving
c. The distance

(4) The SA must be familiar with colors, the variety of colors, and the intensity of the light.

(5) The SA must have the ability to observe objects and incidents in such manner that it will become potential evidence in an investigation.

e. The SA must keep in mind that his senses could fail, and he should know that not all persons will give a detailed description of what was observed, although they are telling about the same incident. The SA must know that the witnesses are telling the truth, but that each person sees things in their own way.

f. To become an expert observer the SA must learn to pay attention and concentrate in particular details in the face and characteristics of an object or scene.

g. When the SA questions a witness about an incident, his questions could be addressed only about what the person remembers and not make suggestions that could influence the description the witness gives.

h. The power to listen well is also required in training. The SA could train his "ear memory" practicing to listen the conversations intently with the purpose of obtaining the greatest amount of information possible. One particular way is to have the ability to listen to sermons in church, school, political meetings, or any speech in a way that after listening to these speeches the SA could later write down in a paper what he listened to.

i. The visual observation training does not require that the SA intently observes all and remember each face or each scene, but, he must concentrate in such details that could be useful in his investigations.

j. Functions of the senses during the observation:

The exactness of an observation will depend upon the senses used to make the observation. You could trust some senses more that others, and the SA must take this into consideration when evaluating their observations. The senses that are used during the observations are:

(1) VISUAL: It is considered as the most precise sense. With just observing some characteristics of a person the SA could complete the image with known facts.

(2) HEARING: This is the most objective sense. When making and observation based in the sound there is not always precision. Frequently, you do not know the origin of the sound or the distance from where it came. The variety of sounds also are difficult to describe. When listening to a sound, the witness normally tries to associate it with some other known sound so as to make a comparison later on.

TACTILE This ~~is a sense? I thought the fifth sense was~~ feel...

(3) TACT: In most people, the sense of tact is not well developed and it must be considered as a limited means of perception. Without the help of a visual perception the sense of tact could confuse us, in such way that an observation in the dark using the sense of tact could be very doubtful. Nevertheless, the sense of ~~tact~~ of the blind persons is well developed.

feel

(4) SMELL: The sense of smell is not to be trusted much. Many things have the same smell and for that reason an observation based on this sense must not be taken very seriously.

(5) TASTE: The sense of taste is not very trustworthy since this sense is very personal and the objective observation of taste is easily replaced by the person's individual sensation.

k. Psychologists indicate that:

(1) 85% of what we learn is through the visual sense.
(2) 13% is learned through the sense of hearing.
(3) 2% is through the sense of tact, smell and taste.

l. Psychological elements of observation:

The SA must know both elements of observation and the observation's psychological obstacles so as to properly evaluate an observation.

m. The observation process in order of occurrence is:

(1) The SA must have the ability to obtain a complete physical description of a person in a few seconds. This ability could be acquired through:

a) Knowledge of the meaning of words used to describe the characteristics.

b) Practice the description of one or two characteristics, such as the eyes and the nose, of different persons and continue this until all the characteristics have been completely studied.

c) Train to define the descriptions in a precise order. Example: from the head to the feet (hair, forehead, ears, eyes, etc.)

n. The SA does not always have time to obtain a complete description of a person, in this case he must concentrate in the following:

(1) Outstanding characteristics, such as moles, scars, lack of an arm, leg or other limbs.

(2) Height
(3) Built
(4) Weight
(5) Age
(6) Race
(7) Sex
(8) Eyes
(9) Hair
(10) Complexion
(11) Nationality or citizenship
(12) Clothes

CHAPTER XXVII

PLANNING AND CONDUCTING A MOBILE (ON FOOT) ~~VIGILANCE~~ SURVEILLANCE ! FIXED VIGILANCE AND PATROL CAR VIGILANCE

INTRODUCTION:

As a counter intelligence (CI) Special Agent (SA) you must know how to plan and conduct a vigilance. It is probable that during your career as a SA you will be assigned to missions to conduct a vigilance. It is your duty to establish the personnel, time and equipment that will be needed to carry out this mission.

GENERAL FACTS:

1. Determine the vigilance objectives:

a. The vigilance is an investigative tool that consists of keeping a person, place or target under physical or technical observation to obtain evidence or information pertaining to an investigation or CI operations.

b. When more simple methods and financial expenditures have not been successful, the vigilance is used to fulfill the specific objectives of the investigation. The objectives of vigilance include:

(1) Establish the identity of the person involved in activities of interest to CI.
(2) Detecting ilegal activities that fall under the jurisdiction of CI section.
(3) Obtain information to use in an interrogation.
(4) Develop leads for future investigations.
(5) Confirm or refute information.
(6) Obtain admissible evidence in a legal manner.

[page missing]

d. Detailed description of the name and addresses of associates, contacts and relatives of the SUBJECT.

e. Professional training of the SUBJECT in the countervigilance techniques (Figure 1).

FIGURE 1
COUNTERSURVEILLANCE

SUBJECT ACTIONS	COUNTER MOVES
Using convoy techniques	Using reserve personnel so they be aware of the convoy techniques
Changing direction many times in a short time	Constant change of watch persons
Re-tracing a course	Constant change of watch persons
Using the reflection on windows	Allow quite a distance and take up innocent actions, such as passing the SUBJECT and entering a store
Using baits (throwing paper or similar objects) and observe if any person picks it up	Use reserve personnel to extract the articles an hour later
Changing the pace as you walk	Maintain harmony with the area and act in a natural way
Using public transportation and immediately getting off	Maintain at least one watch person without climbing on public transportation
Getting off public transportation in a deserted area of	Maintain the vehicle or get off and walk in the opposite direction the SUBJECT
Climbing up various public transportation in succession	Using support vehicles

4. Conduct a study of the area to obtain and analyze detailed information of the place where the vigilance took place. Consider the area where the SUBJECT lives, works or spends time.

a. Obtain a map and take notes of:

1) Road constructions
2) Police control points
3) One-way streets
4) No outlet streets
5) Other articles of potential interest (Shopping centers, markets, etc.)

b. Identify the nature, place, structure and type of building that is most frequently found. Put emphasis in:

1) The residence of the SUBJECT.
2) The working place of the SUBJECT.

c. Study the population of the area to identify particular or potential problems.

1) Race
2) Custom and cultural habits
3) Religion
4) Language
5) Reaction of the people to strangers

d. Identify the traffic pattern

1) Change of workers
2) Movement of vehicles

a) One-way streets
b) Changing directional lines
c) Congested areas
d) Zone considerations (commercial, residential or industrial)

e. Identify the public transportation systems including:

(1) Type (bus, taxi, railroad)
(2) Tolls (cash or special coupons)
(3) Timetable
(4) Loading and unloading places

f. Review the local laws

(1) Identify the local laws and their impact in the personnel and method regarding vigilance.

(2) Identify the application methods.

(3) Identify the local police agencies, including their appearance.

g. Obtain the weather reports during your vigilance.

h. If possible, conduct a search of the area.

5. Prepare a vigilance plan that includes all the operational considerations and instructions to make sure that the objective of the watch is achieved. The plan must be detailed to avoid wrong interpretations, but it must not be so restricted that it eliminates flexibility and the initiative of the individual watch person.

NOTE: The vigilance plan could be formal or informal, oral or written, depending upon the circumstances and time availability.

a. Identify the personnel requirements.

(1) Identify the number and type of persons that would be required.

(2) Select qualified personnel to participate in the vigilance. Main qualifications include:

(a) Previous experience in conducting a vigilance.

NOTE: It is essential that a maximum number of personnel have previous experience in conducting a vigilance, because operational and technical methods cannot be learned completely from a book. A person without qualification could harm the vigilance.

(b) Physical appearance that does not attract curiosity.

(c) Ability to stay without being recognized and ability to mix with his surroundings or environment.

NOTE: Select persons from the area to be used in the area where other persons will attract attention. These other persons must be used to control and supervise the vigilance of a place from a safe distance.

(d) Expedients (ability to adapt quickly to any situation)

(e) Physical vital strength and patience

(f) Detailed perception

(g) Retentive memory

b. Determine the requirements of the logistics and administrative supports.

(1) Relief vigilance personnel from other duties

(2) Obtain special documents, if required

(3) Provide financing to cover the project and for contingent financial expenses

(4) Arrange to obtain the vehicles

(5) Obtain and examine the support equipment

(6) Arrange for food and other commodities, if appropriate, for the vigilance personnel

(7) Prepare one or more cover stories to explain each presence and activities of the watch persons in a particular place

(8) Plan the relief for the watch crew

(9) Give them arms, if necessary

c. Determine the control and communication procedures

(1) Establish the control procedures

(a) Establish a central control point to direct the vigilance operations

(b) Clearly tell the watch personnel what is the chain of command from the watch man to the control point.

(2) Establish the procedures for communication.

(a) Establish radio communications, when possible, as the foremost method of communication between the operative elements and the control point.

NOTE: The use of the safe communication systems could be necessary in some circumstances.

EQUIPMENT AND PROVISIONS

Radios
Cameras and accessories
Binoculars
Tape recorders
Books and pencil
Maps
Small transmitter in SUBJECT'S car
Receiver for the transmitter
Change of clothes

(b) Establish visual signals when the radios do not work or there are no radios available.

1 Limit the number of signals and keep them simple.

2 Visual signals must be natural gestures that do not attract attention to the watch person (Example: taking a paper from your pocket, lighting a cigarette, etc.)

(c) Establish the procedures for emergency communication.

d. Determine the specific mission that will be assigned to each group or individual watch person.

NOTE: The planning and preparation must consider all the possible contingencies that could develop during the vigilance.

6. To direct the members of the team about vigilance.

NOTE: The watch team must know as much as possible about the case so that in such way they could interpret the SUBJECT'S actions.

a. Inform the participants of the vigilance objectives.

b. Inform the participants of the type, methods and techniques that will be used in the vigilance (Figures 3 and 4).

c. Inform the participants of the role they will play in the vigilance.

d. Provide the participants with the target information and the area. Use photographs, maps, sketches to familiarize the participants completely with the target aspects and with the area that will be watched.

e. Provide additional training and preliminary training in the vigilance and counter vigilance methods.

VIGILANCE METHODS

a. A fixed vigilance is when a watch person(s) is kept in a place or fixed position to observe the activities of an specific place.

b. A vigilance in action is when the watch person(s) follow the SUBJECT from one place to another to keep the continuous observation of his activities. The vigilance in action could be:

(1) A mobile vigilance (feet)

(2) A car patrol vigilance

c. A technical vigilance is when technical visual equipment, electronic bugging equipment, and photographs are used.

d. A mixed vigilance is when there is a combination of methods mentioned above. This method is more expensive in money terms and personnel, but will give us the best result.

FIGURE 4
VIGILANCE TECHNIQUES

DISTANCE: The distance between the watch person and the SUBJECT will depend upon the circumstances and the watch person's judgement and must vary during the course of the vigilance. Normally, the more people there are in the street the closer the watch person will be from the SUBJECT.

TURNING ON CORNERS: Do not make immediate turns after a SUBJECT in corners. A suspicious SUBJECT could "examine and observe" a watch person by just standing in the corner and observing attentively these persons that turn around the same corner. Making a wider turn will help keep our pose and will allow us to review the area.

CONVOY: Valuable SUBJECT(s) to a vigilance could use convoys while conducting important activities. The convoys will keep a position in the back of the SUBJECT, keeping him on view, and is alerted about watch persons. Be attentive and alert about the utilization of convoys and take appropriate action to prevent the commitment of the vigilance.

DECOYS: The SUBJECT uses a substitute of similar physical appearance so as to act as a decoy and to confuse the watch person. This is an efficient method when it is used in the residence or work place of the SUBJECT.

CLIMBING BUSES AND TAXIS: If the SUBJECT climbs a bus or taxi, the watch person "A" must try to climb the bus or taxi, but always keeping a distance behind the SUBJECT if possible.

RESTAURANT: Obtain a chair out of the direct SUBJECT'S view range, but so as you can see the SUBJECT, if possible, in a place where you could listen to the SUBJECT. Order according to the type of service ordered by the SUBJECT to be sure that you can pay the bill and leave the restaurant without loosing track of the SUBJECT.

RADIOS: The use of communication equipment must be without attracting attention to the public's curiosity. Do not bend to approach the microphone.

RECOGNIZING THE SUBJECT: The SUBJECT must be physically shown to the watch person, if possible. Study and be prepared to recognize the appearance and the SUBJECT'S mannerisms. Do not depend in the SUBJECT'S dress manner.

VIGILANCE TECHNIQUES

COMING INTO A BUILDING: The size, nature and surroundings are significant considerations to determine future actions. Small buildings, if any, could be kept under vigilance, it is not necessary to follow the SUBJECT to this building unless the SUBJECT made a contact with other persons there in the past. In large buildings, follow the SUBJECT and use the inside of the building to your advantage. Keep in mind that lazy persons attract attention.

ELEVATORS: Follow the SUBJECT to the elevator only if there are other persons and if the SUBJECT does not suspect he is been observed. Stop in the floor above or below the SUBJECT and use the stairs to get to the same floor as the SUBJECT'S. In department stores or similar buildings, the watch person could leave the elevator on the same floor as the SUBJECT. If the SUBJECT enters an elevator alone, stay in the lobby and determine the direction the SUBJECT went to by observing the floor indicator of the elevator. Use the stairs and another elevator to reach the same floor as the SUBJECT'S.

Figure 4 (cont.)

7. Conduct the vigilance using one of the methods mentioned below:

a. The method of a watchman

NOTE: Avoid this method in a moving vigilance, if possible, because it does not allow flexibility.

(1) Operate in behind the SUBJECT and in the same street.

(2) Operate in the street adjacent to the SUBJECT when it is operationally necessary to avoid the commitment of the vigilance. The circumstance will dictate if we must operate in front, behind or next to the SUBJECT. (EXAMPLE: Operate next to the SUBJECT when he turns around the corner to observe if he makes contact or enters into a building).

(3) Keep close to the SUBJECT to observe his actions.

(4) If the SUBJECT turns around in a corner and the area is not too crowded continue crossing the street in the intersection. Observe the street in the direction of the SUBJECT, write down the position and action of the person and act according to the situation.

(5) If the SUBJECT turns around in a corner that is crowded, stop in the corner, in a casual manner and observe the SUBJECT'S actions. Unless the SUBJECT is stopped in a corner, continue the vigilance in the same street.

b. The two watchmen method ("AB" method)

(1) A watchman is kept in position "A" directly behind the SUBJECT.

(2) A second watchman is kept in position "B" behind "A" or in the street next to the SUBJECT and next to him.

(3) The distance is kept according to the situation.

(4) If both watchmen are in the same street and the SUBJECT turns around in the corner, watchman "A" continues to walk in the original direction and crosses the street at the intersection. From the adjacent street, watchman "A" points out the appropriate procedures of following the SUBJECT to watchman "B".

(5) If watchman "B" is operating in the adjacent street and the SUBJECT turns around in the same corner that he is at, watchman "B" must cross the street behind the SUBJECT and take watchman "A"s position. It is not necessary to use signals because this arrangement must be established beforehand.

(6) If watchman "B" is operating in the adjacent street and the SUBJECT crosses the street in the direction of watchman "B", watchman "B" must limit his step to avoid contact with the SUBJECT. Watchman "B" must enter in a store or continue walking straight ahead, keeping visual contact with watchman "A" to look for a signal indicating his next move.

c. The three men method (The "ABC" method).

(1) A member of a group is placed in position "A" at a short distance from the SUBJECT. Watchman "A" observes with detail and writes down the SUBJECT'S actions.

(2) The second watchman is placed in position "B" behind watchman "A". Watchman "B" keeps the constant observation of actions of both watchman "A" and the SUBJECT and prepares to assume the position of watchman "A" when it is required. Watchman "B" also observes to see if there are any convoys and takes appropriate action against these convoys.

(3) The third watchman is placed in position "C" in the street adjacent and next to the SUBJECT. Watchman "C" directs the actions of watchman "A" and "B" with signals arranged beforehand and prepares to assume the watchman "A"s position if the SUBJECT crosses the street and leaves watchmen "A" and "B" alone.

NOTE: If the group of watchmen have more persons, they will follow behind watchmen "B" and "C".

(4) If the subject turns around the corner directly on the side he is walking (out of watchman "C"), watchman "A" crosses the street in the intersection and assumes the position of watchman "C" and watchman "B" places himself in position "A" and watchman "C" crosses the street and places himself in position "B".

(5) If the SUBJECT turns around the corner and crosses the street in the direction of watchman "C", it is not necessary to change positions.

(6) If the SUBJECT simply crosses the street in which he is walking, without turning around any place, then watchman "C" is placed in position "A", and watchman "A" assumes the position of watchman "C" and watchman "B" crosses the street and places himself in position "B".

NOTE: All position changes must be directed depending upon the circumstances and the watchmen judgement and they will be done in a way so as not to attract the attention of the population or the SUBJECT'S attention.

d. The progressive vigilance is used when the SUBJECT has counter-vigilance experience and it is expected that he will use any technique to avoid the vigilance.

(1) Locate the SUBJECT'S place to start (residence, office, etc).

(2) After locating this point, start to pick up the SUBJECT from any place outside out of his sight.

(3) Continue and observe the SUBJECT only at short distances on the first day.

(4) In the following days, pick the SUBJECT at the time and place where you left him the last time, and again follow him at a short distance to a new point.

NOTE: This method will be painful and slow if the SUBJECT changes his daily routine occasionally, but will eventually take the watch persons to the places and contacts that the SUBJECT wants to keep secret.

8. Write down all the observations regarding the SUBJECT and his activities. Write down in a manner that does not attract attention. The small tape recorders are a valuable tool during vigilance. Writing notes in maps or newspapers also works.

9. Carry out the fixed vigilance.

a. Establish an stationary position to avoid the SUBJECT'S detection or the curiosity of other persons. Conduct the vigilance in one of these positions:

(1) A fixed place could be used during a short term or during a stop in a mobile vigilance.

(2) With a parked vehicle in the vicinity of the target.

a) Do not park in the same place for a long time.

b) Warn the police agency if the vigilance involves parking a vehicle for a long time.

c) Do not keep the vehicle's motor running while parked. It is very dangerous (carbon monoxide could enter inside the car) and will attract attention.

d) Unplug the light inside the vehicle.

e) After parking the vehicle, you must open the door and close it, many persons unconsciously listen to determine if they open and closed the vehicle's doors right after parking.

(3) In a room or an apartment located next to the SUBJECT.

(a) This place must be one or two floors above the SUBJECT'S place.

(b) This place must be accessible to entrances that are not visible by the SUBJECT.

(c) This place must be occupied all day to avoid the entrance of non-authorized persons.

(d) The observer must seat in a dark room away from direct view of the window to get the best advantage that the shade in the room offers.

(e) Limit the number of watch persons to two or three in a position, because a larger number could attract attention.

(f) Frequently relieve the personnel to avoid fatigue.

10. Carrying out the vehicle's vigilance method:

a. The vehicle's method.

NOTE: Avoid this method in the mobile vigilance, if possible, because it does not allow flexibility.

(1) Prepare the vehicle.

(2) Operate in the back side of the SUBJECT'S vehicle.

(3) Maintain close to the SUBJECT to observe his actions.

(4) If the SUBJECT'S vehicle turns around in a corner follow him or continue crossing the intersection and make a "U" turn and continue following him. Observe the street and the direction of the SUBJECT, write down the position and persons's action, and act according to the situation.

b. The two vehicle method ("AB" method)

(1) Prepare the vehicle.

(2) The first vehicle is kept in position "A" directly behind the SUBJECT, while this vehicle must be kept at least two or three vehicles behind the SUBJECT'S vehicle.

(3) The second vehicle is kept in position "B" directly behind "A" or in the street parallel the SUBJECT'S vehicle and at his side, while receiving directions, by radio from vehicle "A".

(4) The distance is kept according to the situation.

NOTE: It is possible to keep the vigilance through the back mirror of the watch person's vehicle when traveling in front of the SUBJECT'S vehicle.

(5) Change positions of watch person's vehicles frequently to avoid that the SUBJECT recognizes these vehicles.

c. The three vehicle method ("ABC" method)

(1) Prepare the vehicle

(2) In a vigilance through vehicles using the "ABC" method, the watch person's vehicles are lined in the same manner that in "ABC" techniques for mobile vigilance (on foot). Vehicle "C" operates in a known parallel route.

(3) If the circumstances dictate it both vehicles "B" and "C" could operate in the SUBJECT'S parallel route. Change vehicles "B" and "C" frequently with vehicle "A".

(4) A watchman's vehicle could be placed in a position in front of the SUBJECT'S vehicle to avoid that the SUBJECT could recognize the watchmen's vehicles.

11. End the vigilance when:

a. The vigilance objectives have been attained.

b. The SUBJECT of a discreet vigilance knows that he is under vigilance and takes actions that indicate that he recognizes that he has been watched.

12. Prepare the vigilance reports using the Agent's Report. The report must have the following information:

a. Introduction paragraph

(1) Date and time when the vigilance started and ended.

(2) Identify the person under vigilance, if he is not the SUBJECT of the investigation.

(3) Complete identification of other agencies or person(s) that provided assistance during the vigilance.

(4) Type of vigilance

(5) Specific place or general area involved.

b. Detailed description of the SUBJECT, including his mannerisms, and defined habits.

c. Chronological details of events or activities in a narrative form or tabulation, identifying each contact and building by number (For example, Contact 1); a summary of all the conversations that were heard about the SUBJECT. Including an exact transcript, if possible.

d. Description of each contact.

e. Description of each building implied.

f. If there is a formal report, include the date, time and reasons for which the vigilance was discontinued.

g. The SA in charge of the vigilance team signs the report.

CHAPTER XXVIII

TERRORISM

INTRODUCTION:

In this chapter you may describe terrorism, the phases of the conflict under low intensity, who were the terrorists, the characteristics of the terrorist operations, the terrorist organization, the arms used by the terrorists, the security methods of the terrorist's groups.

GENERAL FACTS:

QUESTIONS TO BE COVERED IN THIS CHAPTER:

1. What are the phases of the low intensity conflict?

2. How is terrorism defined?

3. Who are the terrorists?

4. What are the characteristics of the terrorist's or rebel's operations?

5. How is the organization of a terrorist's movement?

6. What are the methods to provide security to a terrorist organization?

7. What arms are used by the terrorists?

8. What are some of the targets that are most attacked by terrorists?

9. What are some of the most common terrorist activities ?

10. What is the terrorist's goal?

BASIC DATA ABOUT TERRORISM AND REBELLION

THE REBELLION OR CONFLICT PHASES OF LOW INTENSITY:

1. PHASE I: (Latent or Incipient Insurrection) This phase rotates between the circumstances of the subversive activities is only a potential, latent or incipient threat, and situations in which the subversive incidents and activities occur frequently and in an organized way. This does not include a violent burst of activity or chaotic activity.

a. EXAMPLES OF ACTIVITIES THAT COULD BE CARRIED OUT IN PHASE I:

1) The rebels starting from a relatively weak position, plan and organize their campaign and select urban or rural areas of objectivity.

2) The open or clandestine organizations are established. If the insurrection party is ilegal, the organizations will be clandestine.

3) Psychological operations are carried out with the purpose of exploiting complaints and people's wishes.

4) Then the organization starts with a ghost government.

5) Once the party is established, they concentrate in gaining the influence of the population and infiltrating in the government, economic and social organizations, and in presenting a threat to the administrative ability of the government.

6) During the last stage of Phase I the importance of recruiting, organizing and training the armed elements is emphasized.

7) The police forces are attacked, other activities terrorist (groups) and some other military operations of less importance to try to influence additionally over the population, or to provide arms for the movement and confronting the government's ability to keep peace and order.

2. PHASE II: (Guerrilla warfare) This phase is reached once the subversive movement has gained sufficient local and external support and starts to conduct an organized guerrilla warfare, or forms of violence against the established authority.

a. EXAMPLES OF ACTIVITIES THAT COULD BE CARRIED OUT DURING PHASE II:

1) Phase I is continued and expanded. The rebel's political and military control is intensified over the territory and the population.

2) Guerrilla warfare is used in a great scale and in some areas a limited defense is mounted.

3) According to what the situation allows a rebel's government is organized in areas they dominate, and in areas that have yet to be under their control.

4) The most important military goal is the control of the greatest area. The rebels try to understand the government troops in static defense and interdiction operations and they try to destroy the communications lines and take or destroy the government's supplies and resources.

3. PHASE III: (Movement war) The situation advances from Phase II to Phase III when the insurrection has mainly changed to a movement war between the organized rebel's forces and the government forces.

a. EXAMPLES OF ACTIVITIES THAT COULD BE CARRIED OUT DURING PHASE III:

1) The activities that were initiated in Phases I and II, are continued and increased.

2) The largest units in size are used to combat the government forces and gain key geographic and political objectives that will help overthrow the government forces.

3) If the rebels try to win the military sector over and the government is overthrown, immediately they will initiate their consolidation activities. This includes removing the potential enemies, establishing additional control mechanisms and the re-structuring of society.

(4) Additional information and summary of the terrorist's personality: In general, a terrorist is a determined person who thinks that he or she is participating in a dynamic political process but that cannot distinguish the difference between the actions and moral principles; to them the objectives justify the tactics. The true terrorist is not a crazy fanatic as is commonly thought. They are hard-working persons that are prepared to give their lives for the cause. Most terrorists desire to live to see that their goals are fulfilled or carried out; to attain that objective they use persons with mental problems (crazy people) or common criminals to carry out risky missions such as murders.

b. AGE: In general the age of a terrorist is between twenty and thirty years of age. For the local groups is even adolescents. The leaders of any type of organization is commonly older (58, 40, 35).

c. SEX: For the most part in the terrorists' history, they have been predominantly <u>males</u>. During a period of a decade (1966 to 1976), 80% of the operations were addressed and executed by men. The role of a woman in those times was to recount (collect) intelligence, such as messengers, nurses, and the operation of safe houses. From that era on there was a dramatic change in the feminine participation in the terrorist acts. At present, the greatest part of the terrorists are still men, but with a great women participation. The participation of women in terrorist movements is due in part, to social changes, female liberation and youth's rebelliousness.

d. CIVIL STATUS: The greatest part of the terrorist organizations have a majority of single members. The accepted general figure is between 75-80% single. This reflects that marriage is considered as an operational problem for the group. Frequently the members of a terrorist group that are married break up with their family once they find themselves convinced in their group's beliefs and they follow them.

e. ORIGIN: The urban metropolitan areas constitute the source of the greatest part of the terrorist numbers.

f. SOCIO-ECONOMIC HISTORY: Normally they come from liberal party member parents. There is a preponderance of professionals, such as lawyers and doctors, but the other occupations include clergy, business executives, diplomats, government employees, police and members of the armed forces. The terrorist groups usually come from middle and high classes.

g. EDUCATION AND OCCUPATION: There is a vast majority of students and intellectuals within the revolutionary movements and their directors. The majority of the leaders have received some university education or have taken higher education courses and then some. The social and humanity degrees seem to attract many; the students rarely come up as leaders, but the universities are a field for the revolutionary movements.

h. RECRUITMENT: The universities play an prominent role in the recruitment of terrorists. They introduce anarchist and marxists doctrines and many of the student federations are controlled by radicals. The jail adds another element, although it does not play such an important role as the university's.

i. RELIGION: The terrorist tend to be atheists, devoted to violence. This does not mean that all terrorist are atheists. In Latin America's case, the catholic priest's and the nuns have carried out active roles in the terrorist operations of both sectors.

COMPARISON BETWEEN THE TWO CATEGORIES OF TERRORISTS:

	NATIONALIST	IDEOLOGICAL [millennium-oriented]
Personality:	Educated leader Idealist Activist	Same, preponderance of socially unadjusted youth
Age:	From adolescence to the 30's (leaders in their 40's)	In their twenties, thirties
Sex:	Masculine (a few active ones from the feminine sex)	Divided almost 50% women have very active roles.
Civil Status:	Single	Single
Origin:	Metropolitan area	Metropolitan areas
Socio-economic history:	Low and middle class	Middle and higher classes (leaders middle to high classes)
Education and Occupation	Varies greatly (Leaders are professionals)	University and Professional
Recruitment	Varies greatly in cities	City, University, Prisons
Religion	Varies greatly	None

TWO MAIN TERRORIST CATEGORIES: With the considerable changes that have taken place during the last twenty years, there has come into play two main terrorist categories:

a. Nationalist: They take power or cause a national revolution. The control of specific territory is their common denominator. These groups have as principal goal to take a territory as a sovereign entity. They have objectives defined in a short term and frequently make do in a practical manner to attain them.

b. Ideological: Revolutionaries and anarchists of an indefinite ideology that try to destroy the existing system. As a general rule they try to avoid to arouse any definite substitute government because this tends to divide the organization through dissention.

METHODS OF OPERATION: Terrorist operations are being carried out in a professional manner and are executed by well-trained specialized clandestine elements, particularly by international groups. The terrorist organizations are becoming bureaucratic institutions and their members are specializing in diverse areas. There is evidence of one transnational affiliation and assistance between the groups. The terrorist groups generally operate as clandestine organizations.

a. To avoid penetration and information loss about the organization, operations, techniques and plans, groups practice strict security measures. A leader is designated and guided about the mission and the support requirements.

b. Procuring even more security, frequently the members of the team do not meet but until the last rehearsal and shortly before leaving towards the place where the mission will take place. In such manner, the members of the team and the support personnel will not know the location of the target until it is necessary to carry out the mission. The identity of each member of the team will be kept in secret, even from the member themselves, by using names and false identification.

c. To increase security, a special intelligence team will carry out a detailed search of the area or the target. To increase the security even more, many targets that have been recognized will not be attacked by a reason or other, so the fact that a search has taken place does not mean that the target will be attacked. Additionally, to make the hamper or prevent the detection, they plan a greater number of attacks than they will actually carry out.

d. Urban local groups carry out their operations as an initiative of their local cells or their movement's central command.

e. Terrorists normally look to exploit the vulnerabilities, attacking targets that have a weak security stand. Terrorist operations are characterized by: "THE VIOLENCE", "SPEED", AND "SURPRISE". Terrorists reduce their own vulnerabilities to reduce the risk of the operation. If the original target is well protected, they take into consideration the degree of risk and vulnerability of the group, select another target. This does not mean that terrorist groups will not attack a high security target and risk a suicide mission if they think that could be the last resource.

TERRORISTS TARGETS: The terrorists targets are generally of two types: Symbolic or pragmatic. Targets that could serve both purposes are selected if they are available. Targets are more symbolic when terrorists are weak and vulnerable. As the movement grows, targets are more pragmatic. The definition of the two types of targets is as follows:

a. SYMBOLIC TARGETS: Symbolic targets are normally prominent members of a regime or an institution. The terrorist's acts against the target are committed in highly visible places to attract the greatest degree of attention possible and they serve as principal instrument to reduce the trust, inflict fear and provoke the repression of the latter psychological use by the movement.

b. PRAGMATIC TARGETS: Pragmatic targets include multinational corporation executives, key members of the opposition, whose selection has the purpose of coercing the group's objective so as to support the movement; to obtain resources, such as, money, supplies and arms.

TERRORIST ACTIVITIES: The activities of the terrorist groups include:

a. Murders
b. Bombs (including the use of letters and explosive packages, and fire bombs)
c. Kidnapping and taking hostages
d. Pre-meditated fires
e. Ambushes
f. Armed attacks
g. Street tactics
h. Robberies

ADDITIONAL INFORMATION ABOUT TERRORISM:

a. Terrorist goals:

1) Guide the masses not to support the government and support their movement.

2) Terrorism will give the urban insurgent a method to develop the potential for mass uprising and give the rural insurgent a method to oblige them to reduce the control of the government and to force them into the desired behavior.

3) These goals constitute the fundamental terrorist threat for governments.

LOCAL LEVEL ORGANIZATIONAL CHART

<u>COMMAND</u>

<u>INTELLIGENCE SECTION</u>   <u>SUPPORT SECTION</u>   <u>COMBAT ELEMENTS</u>

NATIONAL LEVEL ORGANIZATIONAL CHART

<u>COMMAND</u>

<u>SUB-COMMAND</u>   <u>SUB-COMMAND</u>   <u>SUB-COMMAND</u>

<u>INTELLIGENCE SECTION</u>   <u>SUPPORT SECTION</u>   <u>COMBAT SECTION</u>

LN324-91

CHAPTER XXIX

COUNTER TERRORISM

INTRODUCTION:

In the previous chapter "Terrorism" was discussed in the most important points in regards with the matter of terrorism. Now let us see what must be the government's and the Security Forces answer to the threat of terrorism.

GENERAL FACTS:

There is no country in the world that does not have or could have the threat of terrorism. The act of terrorism is very simple to carry out, but the operations of counter terrorism are not so simple. Counter terrorism requires preparation, training and a special execution: A failure will result in the loss of innocent lives and possibly a victory for the terrorists. Above all, the counter terrorist operations demand good military intelligence cooperation.

THE FIVE COMPONENTS OF A COUNTER TERRORIST PROGRAM:

a. In this space we will discuss the government actions against the terrorist activities. Before we start to discuss the components of a counter terrorist program we must mention the terrorists' goal and the fundamental threat of terrorism to governments.

1) Question: What is the terrorists' goal? And what is the government's goal?

Answer: Terrorists wish to obtain the popular support for their movement. The government wishes to keep the popular support on their side.

2) Question: Taking this terrorists' and government's goal into consideration, Who could remember what is the fundamental threat of terrorism to governments?

Answer: Terrorism will give the urban insurgent a method to develop the potential for mass uprising and give the rural insurgent a method to oblige them to reduce the control of the government and to force them into the desired behavior.

b. A government's answer to the acts of terrorism could cause even more problems if the government does not follow the procedures of a good program of counter terrorism. For that reason it must analyze carefully the needs of a good program of counter terrorism to avoid making exactly what the terrorists wish.

c. Basically, there are five components of the counter terrorism program:

1) PREDICTION: It includes the intelligence operations, and the work of analyzing the threat, the terrorists' power, and the most vulnerable targets. Our knowledge of the characteristics of terrorism and terrorism's strategy will be key parts in this job. EXAMPLE:

"From our study of terrorism we know that there are many possible targets. We also know that it is not possible to know with certainty what will be the next terrorist's targets, but using our intelligence about the terrorists and their goals, we could make a prediction about the most probable targets and this will give us more possibility to protect these targets or react quickly against the terrorists.

2) PREVENTION:

a. Eliminate the causes: It will not be possible to eliminate all the terrorism causes, but at least a government that could show the population that they are trying to better the society's condition will create an environment in which it will be difficult for the terrorists to gain much popular support.

b. DIPLOMACY: This will have much value because it will eliminate the foreign support of terrorists and their sanctuary---but it is very difficult to imagine that all governments will like to eliminate terrorism because some governments are the biggest sponsors of terrorism. (What could give examples of some countries that sponsor terrorism?)

3) DISSUASION: Block the target. Remember that terrorists like to attack targets that are not protected. As we have discussed there are so many possible targets for terrorists that we cannot get complete protection. But the analysis of terrorists could show the most vulnerable targets and then we could give our priority to those targets. Also, frequently, only in few security actions could dissuade the terrorists.

a. Physical security

b. Personal security

c. Security Operations (OPSEC)

d. It is very possible that the best way to dissuade terrorists is to find a high proportion of their detection, conviction and punishment.

4) PREPARATION: Preparing the government forces to react. INCLUDES:

a. Determining authority and jurisdiction

b. Planning the counter terrorism operations

c. Training the counter terrorism personnel

5) REACTION: The appropriate answer to the incident.

4. MILITARY INTELLIGENCE IN COUNTER TERRORISM:

a. We already know the five components of a counter terrorism program. In each one of the components the military intelligence actions are essential.

b. FUNCTIONS OF MILITARY INTELLIGENCE IN THE COUNTER TERRORISM COMPONENTS:

1) Intelligence collection

2) Intelligence analysis

3) Intelligence dissemination

c. THE MILITARY INTELLIGENCE RESPONSIBILITIES:

1) Initiate investigations

2) Confirm information

3) Obtain information sources

4) Give advice to the Commander

d. MILITARY INTELLIGENCE JURISDICTION:

1) Each country is different and you must study the laws of the country in which you work.

e. MILITARY INTELLIGENCE NEEDS:

1) The military intelligence needs in regards to terrorism are infinite. You need to obtain all the information possible about the terrorists, their targets and the surroundings in which they operate.

f. The legal aspects in regards to the terrorism acts and terrorists have to be considered taking into account that the terrorist is a criminal and that he wishes that the authorities initiate repressive actions. This is one of the tactics used by them to obtain a reaction to the government and therefore strengthen their movement.

5. TAKING HOSTAGES AND THE RESCUE OPERATION:

Since hostage taking is the most difficult type of situation, we will discuss a rescue operation in a hostage taking situation to show some details of the government's reaction to the acts of terrorism.

In this situation it is very important that the government have an appropriate reaction. The use of too much force could be worst than any reaction. Remember that often the terrorist's goal is to provoke the government to use inappropriate force. This is especially important in hostage taking cases. In such a situation the government will have to react very carefully to prevent that the terrorists could attain their goals.

There are four rules for a rescue operation:

a. The objective is a rescue mission to save the lives of the hostages--without giving into the impossible demands of the terrorists. In any action taken by the security forces, this objective has importance, even when one has to escape from some terrorists.

b. The rescue team must be of an adequate size and must only use adequate arms to combat the situation. Having too many people in the rescue group will only difficult the operation and give more targets to the terrorists. Always try to use arms that are not lethal, if possible, to avoid killing the hostages.

c. It is important to obtain and use all the intelligence possible from the terrorists, the hostages, the area, etc.

d. The rescue team must have a high degree of professionalism. It must be well prepared to fulfill its mission.

NEGOTIATION WITH THE TERRORISTS:

a. In entering in negotiations or considering entering in negotiations with the terrorists, the following are some options the government has:

1) Give into all the terrorists' demands

2) Deny all the terrorists' demands

3) Controlled negotiation so as to get additional time to take appropriate actions.

b. There are varied opinions and philosophies in regards to negotiations with terrorists; the following are among them:

1) Not to negotiate under any conditions

2) To negotiate to obtain the freedom of the hostages

3) Negotiate with the purpose of gaining additional time to take appropriate action.

CONCLUSION:

The counter terrorism operations are some of the most difficult and frustrating to military personnel. But they are also some of the most common types of operations today and could have great impact in the national life. It is important for you, as members of military intelligence corps, to understand the terrorist's operations their possible effects in the insurrection's war and the counter terrorism programs that the governments could carry out to effectively control the terrorist's threat.

CHAPTER XXX

PHYSICAL SECURITY

INTRODUCTION:

Security, as we apply it to our classified information and defense material, is a very complex theme. In order to better understand the complete theme of security, we have subdivided the theme in three parts: PHYSICAL SECURITY, PERSONAL SECURITY, and DOCUMENT AND INFORMATION SECURITY.

None of these three parts could exist by themselves. During the last chapters we introduced the other two securities; personal and documents. In this chapter we will discuss what is physical security in itself, but we wish that you always keep in mind the other two securities so that you may be aware of the relationship that exists between the three.

So that you may fulfill your security function, you may have to be better prepared for the enemy.

GENERAL FACTS:

1. EXAMPLES OF SECURITY:

   a. Physical
   b. Personal and anti-terrorism
   c. Information security
   d. Operations security
   e. Communications security
   f. Transmissions security

2. DEFINITION OF PHYSICAL SECURITY:

Physical security is defined as "The barrier system that is placed between the potential intruder and what you wish to protect. These barriers could be of five types: (NATURAL, STRUCTURAL,.HUMAN, ANIMAL, ENERGY)."

a. NATURAL BARRIERS: Are those natural topographical characteristics such as rivers, mountains, seas, ravines, cliffs, etc., that by themselves slow down or difficult the entry or access of an intruder to an installation.

b. STRUCTURAL BARRIERS: Are those barriers constructed by man, without consideration to its original intention, that could delay the intruder. Some examples of structural barriers are: walls, floors, doors, windows, locks, fences, etc.

c. HUMAN BARRIERS: The guards, managers in charge of lodging, office workers and workshops workers who intercept the intruder and what he wishes to protect.

d. ANIMAL BARRIERS: Generally dogs such as the German Shepherd, are trained and used as guards.

e. ENERGY BARRIERS: Alarms, protective illumination, any electronic devise that serves to protect an installation.

3. PRINCIPLES IN WHICH THE APPLICATION OF PHYSICAL SECURITY IS BASED:

a. The enemy's agent must have access to the information or material that interests him. The type of access depends in a number of factors, and could be done in different ways:

1) When you are considering protecting information, you should not only consider protecting the physical access, but the access to discussions about these material through the use of clandestine devices to listen [bugs]. If the enemy tries to tape a conversation about an specific theme, this is so useful to him as the original document in paper.

2) You must be careful also with the use of long-range photographic equipment to get access through openings in structures.

3) The themes discussed above could be considered also for sabotage. The sabotage agent does not have to place the device or destructive material in the place he wishes to cause damage. He could, in many ways, throw an explosive device against its target, (riffle, grenade launchers, rocket launchers, camouflaged explosives sent through the mail or with supplies), or could contaminate the fuel or oil deposits to cause damage to machinery, although they keep away from him.

4) You may consider all available resources that the enemy could access, and all these must be evaluated to determine how we could be able to counter arrest it.

b. IS THERE ANY IMPENETRABLE BARRIER?

1) ANSWER: There is no barrier that is impenetrable. If a hostile government is set to dedicate sufficient time, money, personnel, materials and imagination to cross a barrier, they may succeed.

c. SECURITY WITH DELAY DEFENSE SYSTEM:

1) Although no barrier could totally exclude an intruder, it could give a determinate delay time. It all depends upon the intruder's ability.

2) Instead of trying the exclusion through the use of just one barrier, the security could be based in a security in-depth system or accumulated delay.

3) To get optimum results it is necessary to add barrier over barrier, delay over delay, until sufficient delay time is accumulated that will allow us to control any possible penetration. This delay should be enough so that the available personnel could neutralize the intruder.

4) A fence without guards allows a short delay. If that fence is patrolled by trustworthy guards that keep it under observation within the delay time, the total delay time increases significantly.

5) In some cases it is necessary to differentiate between the need of denying access and the need to have knowledge that access has been gained. This refers to the neutralization, if a material is committed, you may take action to void its value for the enemy.

6) Physical security must be applied not just as a dissuasive means against the stealing property but also as a dissuasive means against espionage.

7) The spy only partially satisfies his purpose when he acquires information. Information looses value if the persons responsible for its custody know about the leak. Espionage does not have any value if it is revealed.

8) These considerations make the surreptitious entry the greatest danger from the CI's point of view. This makes the creation of two types of barriers necessary. One to protect those things that could be stolen and could not be neutralized and another to protect those things that could be neutralized.

9) To protect those things that could be neutralized a barrier that shows evidence of having penetrated is created. Example: (Broken window, etc.).

d. Each installation must be treated as an individual entity when planning security. The location of an installation alone will bring problems that differ from those aspects of other installations. Each one must be considered as a separate problem.

4. PHYSICAL SECURITY ASPECTS:

DISCUSSION OF DIFFERENT BARRIERS:

a. NATURAL BARRIERS

1) ADVANTAGES OF NATURAL BARRIERS

a) They provide a protection system without additional cost to the installation.

b) The difficulty to penetrate an installation increases according to the barrier.

2) DISADVANTAGES OF NATURAL BARRIERS:

a) Trees, ravines, vegetation, could serve as a hiding place to any possible intruder.

b) Installations that have as barrier a body of water could be subject to penetration through a team of divers.

3) BODIES OF WATER AS BARRIERS:

a) ADVANTAGES:

(1) When the surface of the water is calm, it offers the guards or security personnel a very extensive field view range.

(2) Water offers much resistance to a vehicle used by intruders by making it almost impossible to have rapid access to the installation.

(3) To gain access, the task of hiding a vehicle or boat without been detected by the guards or security personnel will be an obstacle to the intruder.

b) DISADVANTAGES:

(1) When the water is agitated it reduces the field of vision of the guards or security personnel.

(2) It is possible to control the movement of a vehicle or boat to keep it hidden between waves.

(3) The surface of the water reflects the light given by the illumination system. An intruder may use this situation in their favor when trying to penetrate an installation.

4) THE LAND AS BARRIER:

a) The land where the installation sits must be evaluated and considered as much from the surface access point of view as from below the surface.

b) Points to consider when evaluating the land as barrier:

(1) The looser the ground the more noise it will cause when the intruder walks.

(2) Muddy soil without vegetation is very difficult to cross and at the same time the intruder leaves their footprints.

(3) Light colored soil provides reflection and contrast so as to allow the most efficient use of natural and artificial illumination.

(4) Land that is uneven such as cliffs and ravines are difficult to cross and limit the amount of equipment and material that the intruder could introduce in the exterior perimeter area.

b. STRUCTURAL BARRIERS:

1) As explained earlier, structural barriers are man-made constructions. To remove the vegetation around an installation is also considered as an structural barrier.

2) FENCES: Fences are independent structures, generally in a vertical plane, designed for the physical and or visual control of access to external areas.

a) General facts about fences:

(1) Define the area they protect

(2) Reduce the number of guards required and facilitate the tasks of the patrol corps.

(3) Cause delay in case of an intent to penetrate

(4) Although they don't deny the access in themselves, they are a psychological obstacle to a possible intruder

(5) They deny accidental access to innocent persons to the protected area

(6) They help control the flow of vehicles towards those entrances controlled by guards

3) TWO TYPES OF FENCES:

a) SOLID: They are used to deny visual and physical access to non-authorized persons. The materials normally used are bricks, concrete, wooden boards, stone, etc.

(1) ADVANTAGES OF SOLID FENCES:

(a) They are useful when you wish to hide certain activities within the installation.

(b) They avoid the possibility of passing small items through the fence.

(c) They could be built in such manner that it would be difficult to cross them without being detected.

(d) For the most part, fences are built of stone, brick and concrete and they extend below the ground and make it difficult to the intruder to penetrate below.

(2) DISADVANTAGES OF SOLID FENCES:

(a) It is difficult to illuminate the zone around the installation because of the shadow caused by the fence.

(b) They do not allow patrols within the installation to observe the activities in the external perimeter.

(c) The installations that use solid fences have guards in towers. Tower guards are a disadvantage in itself. The towers confine the guard in a very limited area. Since the guard cannot move for a long time in the tower he does not stay alert.

b) COMPLETE VISION FENCES: Are built in such manner that they allow visual observation through the entire fence. It is designed only for the control of physical access between two areas.

(1) ADVANTAGES OF COMPLETE VISION FENCES:

(a) They allow the effective use of illumination since they do not cast a shadow.

(b) They allow the effective use of guard patrol, since they could keep the installation's surrounding area in watch.

(2) DISADVANTAGES: They allow a possible intruder to carry out a reconnaissance of the camp and could establish the installation's pattern of internal security guards.

3) PENETRATION: It is the main objective of all enemy or terrorist to attain access to the internal perimeter of an installation to carry out his mission.

4) THREE WAYS OF PASSING THE FENCES:

a) ON TOP: Most fences are not high and are easy to climb.

b) THROUGH THE MATERIAL: (If it is not a solid fence).

Many fences are built in such manner that it is easy to break or separate them in such manner that it will allow the enemy's access without leaving evidence that there was a penetration.

c) BELOW: If the fence is solid and very high, digging and penetrating below is possible.

5) CHARACTERISTICS OF FENCES:

a) The minimum height of a fence is eight (8) feet. This is due to the consideration that an average man could jump or climb that height.

b) It must be extended below the ground level.

c) If it does not extend below the ground level, the minimum space between fences and the ground must not be over two inches.

d) Support posts:

(1) Wood: Must be the best wood quality and measure at least 4 inches wide.

(2) Metal: Must be at least 2 inches in diameter. They must be placed over concrete or firm ground at a depth of three feet.

e) Protection - Upper part of the fence:

(1) All fences must have in the upper part, additional obstacles that could prevent or delay the enemy's penetration.

(2) Complete vision fences:

(a) Barbed wires are placed in metal arms that extend outward, at a 45 degree angle.

(b) Place barbed wires in metal arms in "V" shape.

(c) The arms must be two feet long with three rows of barbed wire over them.

(d) You may also use folding wiring.

(3) Solid Fences:

(a) You may use the same system as complete vision.
(b) You may add glass in the upper part.
(c) You may place sharp metal bars.

(4) DISADVANTAGES: You must understand that the barbed wire system in the upper part of a fence does not completely prevent an intruder's entry. What this system provides is delay to the intruder and is another obstacle that he should pass through.

f) GATES IN THE FENCES: The number of gates in a fence must be limited to the minimum necessary for the efficient and safe operation of an installation. Although all the gates must have the ability to be locked, when locked they must provide the same level of security that the fence itself provides. When there is considerable traffic on foot and vehicles it is preferable to provide separate gates for each type.

g) OPENING IN THE FENCES: All the openings within or below the fence (gully, sewage) that measures over 96 square inches must be sealed in such manner that they could only be penetrated from within. In the case of rivers or ravines that flow in the surroundings of the fence do not allowed this to extend over the water and it must be built parallel to the ditch. In case that fences are built through rivers or ravines, these must be dug to the river bed so as to avoid penetrations below the water.

h) MULTIPLE FENCES: Multiple fences are formed by two or more parallel fences used in conjunction to form a perimeter barrier. In addition to increasing the delay time, they tend to trap the intruder and prevents our personnel from accidentally coming in contact with the alarms or security measures imposed around the fence.

(1) The minimum rules for a fence also apply to each multiple fence unit.
(2) The multiple fences must be at least 10 feet away.
(3) The maximum distance allowed between two fences is determined by the ground, the illumination, and the guard's abilities, but it must not exceed 150 feet.
(4) A greater distance than this, prevents the fences from being completed and could be attacked by the intruder as they treat it as a separate obstacle.

6) CLEAR ZONES: The clear zones is the area of the external or internal perimeter of the installation which is free of obstacles, structures and vegetation.

CHARACTERISTICS OF THE CLEARED ZONE:

a) Must extend throughout a minimum of 20 feet in the external perimeter of the installation.
b) Must extend throughout a minimum of 50 feet in the internal perimeter of the installation.
c) Must remain free of vegetation, structures, trash or any other material that could allow the enemy to use it as hiding place.
d) There should be no trees next to a fence. The enemy could use a tree to reconnoiter the installation and to try the access over the fence.

e) It is important to keep the grass mowed around the cleared zone so that there will be no possible hiding place for the enemy.

f) Do not use the cleared zone as a storage area.

g) If you do not have an adequate cleared zone, you must increase the height of the fence.

h) If a fence is used to protect a large area, if possible, build a perimeter road that allows the car patrols and the quick delivery of reinforcements to any point of the fence.

c. HUMAN BARRIERS: (THE GUARDS AND THE GUARD SYSTEMS)

1) The physical security depends upon the use of guard systems in such a way that natural and structural barriers could be used to control and avoid the access of non-authorized personnel.

2) The guard system is the most important element of the security program of an installation.

3) FOUR BASIC FUNCTIONS OF THE GUARD SYSTEM:

a) Detect the intruders
b) Sound an alarm
c) Capture non-authorized personnel
d) Identify authorized personnel

4) TWO GUARD CATEGORIES:

a) Those whose only mission is to serve as guards in the installation. These men are trained specifically to carry out this task.

b) Those who carry out this task as a punishment or as additional task of their normal work, or it is the job that they have been properly trained for.

5) RECRUITING THE GUARDS: Due to the important role that they play, security guards must be very carefully chosen.

ELEMENTS TO BE CONSIDERED WHEN SELECTING GUARDS:

a) Experience
b) Training
c) Must be strong
d) Must be in good physical health
e) Must be trustworthy

6) TRAINING THE GUARDS:

THEMES TO INCLUDE IN TRAINING:

a) A general orientation that includes the orders and the authority
b) Instructions about the traffic control
c) Riot control
d) Personal defense
e) Arms handling including maintenance and security
f) First aid
g) Communications
h) Use of special arms
i) Plans and emergency procedures
j) Counter espionage
k) Counter sabotage

NOTE: The responsibility of the training generally falls upon one of the members of greater seniority of the guard's forces.

7) THE USE OF GUARDS:

a) The guards' barracks must be located where they could enforce maximum control over the guard's posts and the sensitive areas. They must use the following rules:

(1) In small installations with one only entrance, the barrack must be near the entrance.

(2) In large installations a centrally located barrack is preferable to facilitate the quick deployment to any dangerous point.

b) For the perimeter's security, the most effective use of guards is in fixed points that support themselves mutually. These require that each guard be visible to the one next to him, sharing therefore the responsibility of the area they protect. These posts must also be protected by the elements; such as: wind, rain, cold weather and the sun.

c) It is less costly to use the guards on foot or mounted guards. The guards could verify the barriers at irregular intervals and will make it more difficult for the intruder to penetrate the barrier.

d) No matter what method you use for the guard's service you must prepare orders for each post and patrol. These must:

(1) Must be brief and easy to understand
(2) Include instructions about all the possible contingencies in regards to actions during emergency situations

e) A guard must have sufficient time to rest if the job must be done effectively. Must, at least, be relieved every eight (8) hours. The guards in fixed posts must be relieved each four (4) hours.

8) SUPERVISION OF THE GUARDS:

a) The continuous supervision is necessary to make sure that the guards are in their posts and carrying out their security tasks. The supervisors must keep in contact with each post, at least four (4) times a day.

b) A characteristic guard force must consist of:

(1) A commander
(2) His assistant
(3) Administrative personnel

c) If guard services are given 24 hours, three shifts must be needed. Each shift has a similar organization.

d) The supervision starts with a personal inspection of all the guards before the start of their shift. Each inspection includes:

(1) Personal appearance
(2) The equipment
(3) Knowledge of special orders

9) THE GUARDS' EQUIPMENT:

a) Distinctive uniform
b) Credentials and or appropriate identification as a guard.
c) Appropriate arm
d) Additional equipment: notebook, whistles, flashlights

10) COMMUNICATIONS AMONG GUARDS:

a) Fixed posts and patrols joined by a communications network.
b) Direct telephone may be used.
c) Portable radio.
d) Emergency communications depend on messengers.
e) The vehicles must be equipped with radio-transmitters, receivers.
f) The central station must be in charge of a supervisor.
g) The patrols on foot could use radios.

d. ANIMAL BARRIERS:

1) An animal barrier consists of an animal that is used as guard system.

2) In theory, you may use many types of animals but we have limited the use to a dog, almost exclusively a German Shepherd.

ADVANTAGES OF USING DOGS AS BARRIERS:

1) Their sense of smell and hearing are much more developed than in humans.

2) They have an incorruptible character.

3) They are loyal.

4) They are plunderers by instinct, their qualities as guards are natural in him, and take precedence over their own welfare.

5) The man-dog team is the most effective method in the use of dogs as guards.

6) You may place dogs in open areas where it is necessary to limit movement.

DISADVANTAGES:

1) They lose their effectiveness if they work where there are many people.

2) You could not use it near a road, since the traffic noise will distract him and cause him to lose concentration and effectiveness.

3) They must work at least 75 to 100 yards from a road, or from areas with frequent traffic.

e. ENERGY BARRIERS:

1) An energy barrier is the use of mechanical, electric, or electronic energy to prevent or alert about an intruder's entry.

2) Two important energy barriers are:

a) Protective illumination systems
b) Protective alarm systems

3) PROTECTIVE ILLUMINATION:

a) It is used to increase the guards' field of vision, providing a visual field during the night in areas of poor or any natural light.

b) DISTINCTION OF SILHOUETTES:

(1) When the possible intruder uses dark clothes, he may hide behind the structure's shadows. To aid the guard in distinguishing these silhouettes you may:

(a) Direct additional illumination to the structure's grounds and walls.

(b) You may paint stripes or angles on the walls, fences and structures, that will allow the guard to detect movement.

c) ILLUMINATION OF ENTRANCES: This is a special task since:
(1) Provides illumination to:

(a) Inspection of passes
(b) Inspection of Identification cards or badges

(c) Inspection of vehicles
(d) Inspections of trucks and loads
(e) Illumination of the area surrounding the sentry box

(2) There must be illumination in an area approximately 50 feet around the sentry box, 25 feet as a minimum.

(3) The area inside the sentry box must be kept as dark as possible. In that manner the guard could see the persons, and the persons could not see who is the guard, nor how many guards there are inside the sentry box.

d) SENTRY TOWERS:

(1) The sentry towers must not be over 1,000 feet of distance from one another. The reason for this is that a person with normal vision only has a field of vision of 500 feet in which he could distinguish silhouettes.

(2) The sentry towers must have flood lights, in addition of providing illumination, they must also blind and surprise the intruder, disorganizing therefore the possible attack plan.

e) ILLUMINATION OF VITAL AREAS:

(1) Examples of vital areas:

(a) Communications
(b) Warfare equipment
(c) Water tanks
(d) Energy plant

(2) The vital areas that are considered vulnerable from a large distance must be kept dark.

(3) Vital areas that are vulnerable at short distance must be kept well illuminated.

(4) Other areas that must be kept well illuminated are:

(a) Inactive areas: where there is no night work, areas that provide hiding places to intruders.

(b) Buildings: Illumination around the buildings is necessary to avoid that intruders come in through low windows on the first floor.

(c) Parking area: In addition to providing a good hiding place to the intruder, is a good area for assault to employees of the installation.

f) EMERGENCY ILLUMINATION:

(1) There must be an independent-backup system of illumination when the normal energy source is interrupted. This may be:

(a) A system of floodlights that operate on batteries.
(b) A generator
(c) A central battery system

5. PERSONNEL CONTROL AND IDENTIFICATION:

a. IDENTIFICATION:

1) The most effective manner will be if the guards could personally recognize all the persons authorized to enter the installation.

2) A modified identification system could be used only at the military installations where only military personnel work. A commander could take his unit to the door and become responsible for them.

3) The artificial identification is the most widely used at present. The authorized personnel receives passes or cards where access to a determined installation or activity is authorized. These could be falsified and therefore they must be laminated and prepared with a complex background so as to make falsifying difficult.

4) They must have the photograph of the person, name, and date of birth, height, weight, hair color, color of eyes, sex, name of the installation, rank, title, and signature of the authorizing official.

5) When artificial identification is used, this must execute a rigid control over the devices used.

b. USING THE ARTIFICIAL IDENTIFICATION SYSTEM:

1) The employee receives a card or identification that they keep. When they enter the installation they show the card and come in. This system is used widely but it has its flaws. These are the loss of cards and possible falsifications.

2) In another system, two cards with the same information is prepared.

a) When the person comes to the installation, they give the card that he keeps and he receives another one to be used inside the installation. If one of the two has been altered, the guard could detect the change when he has the two cards in his hands.

6. CONTROL OF VISITING PERSONS:

a. The control over the visitors depends in how sensitive the installation is.

b. Possible visitor's controls:

1) Escorts
2) Programmed visits
3) Visitor's registry
4) Passes for visitors

7. CONTROL OF PACKAGES:

a. You must provide for the search of packages that come in or that are taken out of an installation.

b. If necessary, you may prohibit carrying packages to the installation all together.

8. PHOTOGRAPHS:

a. You must be careful in the areas where classified material is kept to avoid the taking of non-authorized photographs.

b. Generally, only photographers authorized by the information office, or by the commander of the installation could carry cameras to the sensitive areas.

9. VEHICLE IDENTIFICATION CONTROL:

a. Jointly with the personnel control, there must be a control of vehicles.

b. An identification system which identifies the vehicles with authorized access to the installation.

c. It is required that the entire personnel registers their vehicles with the guard's general headquarters.

d. When the registry is done, you may give the vehicle's owner a decal that must be placed in the vehicle's windshield.

e. The declass must be renewed annually and must be rigidly controlled.

10. FIRE-FIGHTING INSTALLATIONS:

a. Fire is one of the most effective tools used by the sabotage teams.

b. Without knowing the cause, a fire could neutralize an installation completely.

c. The security program must include the adequate installations to fight fires and a program for the prevention of fires.

d. COMPONENTS OF A FIRE-FIGHTING INSTALLATION:

1) PERSONNEL: They may civilians or military men. They must be trained adequately in combat and fire prevention.

2) ORGANIZATION: It is a function of engineers. The engineer of an installation serves as commander of the firemen's corps.

3) THE EQUIPMENT: The firemen's ability depends upon the equipment they have. To determine the type of equipment necessary, you must understand the classification of the fires:

a) CLASS A: Are those which consist of common fuels such as wood, paper, and similar materials. Water is the best element to fight such type of fire.

b) CLASS B: Are those of the oil or gas type. Water does not work to put out this type, since water spreads this type of fire. Carbon dioxide is appropriately used to put out this type of fires. Foam extinguishers are recommended.

4) ALARMS: There are two types of alarms: Central and local. They could be automatic and manual. Their placement serves to alert the fire fighters corps and the personnel at the same time.

5) RESERVE FORCES: It is advisable to have a reserve force that consists of personnel trained in the same manner as the main corps.

6) PREVENTION OF FIRES: The entire personnel in an installation has the obligation to participate in a prevention program. You must have a training program so that everyone is conscious of their responsibilities.

7) PLANS IN CASE OF FIRES: You must prepare specific instructions for the entire personnel. You assign specific responsibilities to the entire personnel that is present at the time the fire breaks out.

11. COMMUNICATIONS:

a. A security program must include provisions about communications security.

b. The communications center must be designed as a restricted area and must enforce strict control over the access to this area.

c. The communications center must be located in an area or building that could be easily defended, with some type of protection against aerial attacks.

d. The maintenance and service personnel have a very sensitive position and therefore must have the security authorization according to the sensitivity of the installation.

12. GENERAL SERVICES:

a. There must be provisions that guarantee that electricity and water services are protected adequately and there are emergency sources available:

1) ELECTRICITY: If an installation has its own energy plant this must be located in a restricted area and only authorized personnel should be allowed inside. A barricade system must be built to prevent the entrance of non-authorized personnel.

2) WATER: If the installation has its own fire fighting station, you must give the same protection as to the energy plant. You must protect the water from contaminations.

SUMMARY:

We have discussed some of the measures that could apply in an installation or activity to prevent non-authorized access to these. You must not suppose that these are the only available measures when making a recommendation to a commander during the course of an inspection or carrying out a study of physical security. The minimum rules that have been presented are preferred but are not always possible. Frequently, you may improvise to compensate for the lack of security that results when the minimum rules are not carried out.

Keep in mind that there is not such thing as an impenetrable barrier. One must not depend solely upon natural and structural barriers. The key to the good functioning of any security system is personal efficiency. The barriers that are used only serve to improve the effectiveness of the guards and make the detection of intruders more possible.

The physical security is not the only answer to the commander's problems in regards to security. Unless he has a good personnel security program and a good information security program he would not be successful in his intents to safeguard the information and the classified material of his installation. If there is a flaw in the security system, the intruder takes the necessary key to neutralize the whole security program. Remember this when analyzing an installation during a security inspection.

ANNEX A

PHYSICAL SECURITY REPORT

(Name of the group preparing the study)

TITLE: SECURITY STUDY OF (Name of the installation)

I. HISTORY:

A. The study of security was conducted during the period between (the times and dates) .

The following agents from (designation of the unit that conducted the study).

1. Last name, first name of agent(s) in charge

2. Name

3. Name

B. MISSION OF THE UNIT OR INSTALLATION:

1. The unit ______________________________ has the following mission.

2. Factors that affected the level of security.

a. Discuss the mission of the unit as it affected the required security level.

b. Discuss the location of the unit.

c. Discuss the number and the name of similar installations.

d. Discuss the security classification for information and/or material.

e. Discuss the general importance of the unit studied.

C. LAST STUDIES AND SECURITY INSPECTIONS:

1. Security study: (Date)

2. Security inspection: (Date)

D. UNIT MAPS:

1. Sketches of the unit or installation.

2. Map of buildings (Annex "A" convincing document number ______)

II. MILITARY SECURITY SITUATION:

A. PHYSICAL AND MATERIAL SECURITY:

1. Natural barriers and exterior influencing factors:

a. Topographic description

1) Location of the installation or unit.

General limits:

a) North
b) South
c) East
d) West

2) Ground characteristics

a) According its shape (flat, mountainous, etc.)

b) According to its coverage (clear, etc.)

c) According to its contents (clay, etc.)

3) Type of terrain:

a) Natural:

(1) Hills (location, height, characteristics, photographs)

(2) Ravines

b) Artificial:

(1) Canals, (location, width, depth, photograph, etc.)

(2) Water collectors

b. Immediate areas:

1) Unit, location at ______________________areas pertaining to ____________________surrounded by the following inhabitant groups.

a) Inhabitant groups

-- Population (distance, characteristics, etc.)

-- Settlement (main characteristic of the sector)

b) Educational establishments

-- Schools

-- Colleges

c) Social organizations

-- Number (location, distance, objectives)

-- Leaders (names, last names, identity number, place, address, telephone, etc.)

d) Industries

-- If any (description)

e) Entertaining places

-- Restaurants, billiard rooms, taverns, etc. (characteristics)

f) Crime rate in the zone

-- Common crimes in the zone

-- Police history (rubbery, crime, etc.)

g) Groups with ideologies contrary to the constituted order or power.

-- Investigations to ideologies that could affect the security of the National Unit.

h) Foreigners

-- Names
-- Occupation
-- Nationality

c. Critical zones

1) Are the following installations:

a) Generators
b) Electricity control
c) Water measures
d) Fuel deposits
e) War materiel

2. Artificial barriers

a. Perimeter barriers

1) General Facts

a) The unit borders with walls from north, south, east and west, extension, fencing, type of concrete.

b) The limits of the installation are:

-- North
-- South
-- East
-- West

2) Fences

-- The unit has barbed wire fences, etc. to the north, south, east and west, etc., describing direction, extension, type of fencing or barriers they have (include a photograph).

3) Entrances

-- There are the following entrances in the unit:

-- A door (characteristics, measures, role)

-- An entrance (characteristics, measures, role)

-- Other doors (characteristics, measures, role)

3. Human barriers:

a. Guards and security systems

1) Guard personnel

a) General description

b) Guard service

2) Inspection and control of the guard

a) Inspection system

b) System for its control

3) Use of guards

-- Positions, if there are or are not enough

4) Guard's equipment

-- Disposition of armament, ammunition, equipment, etc.

b. Control and identification of persons

1) Personnel in charge of control

2) Systems for control of persons

3) Identification cards for persons

4) Plant personnel (working inside the installation)

5) Visitors

6) Authorization to access the installation

7) Schedule of access

c. Control of identification of vehicles

1) Registry and control of vehicles

2) Visitor's vehicles (parking area)

3) Systems for inspection of vehicles, entering and exiting)

4) Illumination of perimeter (if enough, photograph)

d. Security of the inside area

1) There is no security

2) The unit has _______ (description of installations)

3) Built by_________ (description of rooms, floors, etc.)

4) The main doors to buildings are ____________.

5) The windows ________________.

6) The upper part, doors, windows, etc., (in regards to security)

4. Animal Barriers

a. If any (type and description)

5. Energy barriers

a. Illumination system

1) If any (characteristics)

b. Alarm system

1) If any (characteristics)

c. Services

1) Electricity

a) Who supplies it

b) Is it enough or not, etc.

c) Water pressure

d) If water supply is enough or not

e) Uses

f) Water tanks

-- Description, characteristics, use, location, etc.

g) For emergency cases, if there are any other sources or own places for collection of water.

d. Special cases

1) Fire fighting systems

a) Fire personnel

-- Plan to put out fires

-- Distance from firemen

-- Composition of firemen corps

-- Equipment used

-- Time to reach the unit if notified of a fire.

b) Fire-fighting equipment available at unit

-- If any (description and location)

c) Fire alarms

-- Description, auxiliary, etc.

d) Water

-- If the unit has water hydrants in case of fire.

e) Counterintelligence plans

-- If any

2. Plan for defense of the camp

a) If any

B. PERSONNEL SECURITY:

1. Main personnel in the unit

Infantry, military intelligence, administrative, civilians, etc.

2. Number of persons

a. Plant personnel

1) Plant number

2) Troop personnel

3) Recruited personnel

3. Civilian employees. (identification and authorization cards, schedule of entrance and exit)

a) Doctors

b) Nurses

c) Secretaries

d) Workers

e) Etc.

4. Others

a. Address of personnel in the general area.

b. Use of mobilization. (If there is any plan for mobilization of personnel in general in case of emergency)

c. Investigation

1) If there have been any suspicious sinister activity, that is, sabotage.

2) If there have been intention to cause fire.

3) Any illegal authority that has been registered.

d. Moral

1) Moral problems that affect the security

2) Military personnel accusations (when a military man reports to his superior about any comrade)

3) If there is a registry of damages or lost material

4) Hatred among military or civilian personnel

e. Personnel identification control

1) Personnel identification method

-- If none, if they intend to have one

2) Visitor's control

-- If none, if they intend to have one

C. DOCUMENT SECURITY:

1. Existing situation

Summary of percentage (%) of documents and classification (ULTRA-SECRET, SECRET, CONFIDENTIAL). If there is no existing classification of documents, if they wish to establish a system.

a. Preparation and reproduction:

1) The sections create sensitive or classified material

2) Precautions with paper ribbons, carbon paper, etc.

3) Document file. (location, adequate or not)

4) Destruction of documentation

5) Access to sensitive dependencies or secret documents

b. Classification and marking:

1) Markings should be placed in documents classified as:

a) Photographs

b) Film

c) Recordings

d) Letters

e) Drawings

f) Maps

2) They are properly stored

3) They are of easy access

-- Manner in which they are stored

c. Re-classification of (classified documents)

1) If they have a higher echelon in each one of the cases

2) Registry and file of classified documentation

3) How the material is filed; ULTRA-SECRET, SECRET, CONFIDENTIAL.

4) Description of building where it is filed

5) Who files in each dependency

6) How long does it take for a person to do that work

d. Transmission

1) Verbal or written communications

2) Using military mail or other mail

3) Stations and telephone numbers and extension numbers

4) They use wire methods, such as telephone, radios, etc.

5) Messengers

a) Who are they

b) It is always the same person

c) They receive instructions for the fulfillment of their work.

e. Dissemination

1) Who authorizes the handling of classified documents?

2) If documents are taken out of the office. Who gives the authorization.

3) They keep the key to the files when they leave the office.

4) Who has that key?

5) If classified documents are taken out, if they need a receipt. If they require previous authorization from their chief.

f. Message center

1) If there is:

a) Description and functioning

b) File description

c) Well or poorly attended

2) Facilities for storage of documents

a) Manner of storage

b) File style

c) Security keys

3) Receipts:

-- System for receiving documents

4) Incineration:

a) There are systems for incineration

b) Where does the incineration takes place?

5) Evacuation:

a) Evacuation plan

b) Vehicles

c) Assigned personnel

d) Priorities

e) Evacuation place

f) Security measures

g) If the classified material is identified

D. SECURITY OF TRANSPORTATION AND MOVEMENT:

1. History

a. They is a topographic chart of the place.

b. Transportation of the installation's personnel

c. Capacity for military transportation or supplied civilians.

2. Aspects to consider:

a. Coverage measures

1) If identity of installation, unit, or part of the vehicles is known

2) Has signs, direction signs or posters

3) Vehicle or continuous transit and uniformed personnel

4) Principal or alternative roads

5) Main roads:

a)______________towards unit
b)______________towards unit

6) Alternative roads:

a)_______________.
b)_______________.

b. Personnel and or security or protection means

1) If any

2) Technical transportation security measures

3) Vehicles that are used in transporting the installation's personnel.

a) Vehicles

b) Buses

c) Civilian buses

III. PHYSICAL SECURITY

A. Deficiencies found in the Study of Physical Security, conducted previously, that could have effect over personnel security and the security of documents.

1. Deficiency: ________________________________.

Recommendation: ________________________________.

2. Deficiency: ________________________________.

Recommendation: ________________________________.

B. PERSONNEL SECURITY:

1. Deficiency: ________________________________.

Recommendation: ________________________________.

C. DOCUMENT SECURITY:

1. Deficiency: ________________________________.

Recommendation: ________________________________.

D. SECURITY OF TRANSPORTATION AND MOVEMENT

1. We recommend to give the installation:

a. Transportation vehicles

1) Buses

2) Ambulances

3) Jeeps (trucks)

4) Loading transportation

b. Coverage.

1) How could the unit cover the vehicles and their movement through a false story if possible.

2) Access roads to the installation.

-- Main entrances for vehicles, pedestrians, etc.

3) Helicopter room

-- Where it could be possible

4) Parking room

-- Owned vehicles

-- Visitors' vehicles

-- Civilian vehicles

5) Security and protection personnel for the vehicles.

IV. ORIENTATION FOR EXIT

A. All the findings and recommendations were discussed during an orientation with unit members:

(Name the participants in the group, with rank, last name, name, initials, role)

1.______________________________.

2.______________________________.

3.______________________________.

V. ANNEXES:

"A"	Convincing document no. 1	Photograph
	Convincing document no. 1	Legend

"B" Physical Security:

Convincing document no. 1 Photograph

Convincing document no. 2 (Description)

"C" Personnel Security:

(Name the documents in the same manner than the ones above).

"D" Document and information security:

Convincing document no. 1 XXXXXXX

"E" Security of Transportation and Movement:

Convincing document no. 1 XXXXXXX

---

1. SUMMARY: (Study of Physical Security)

2. CONCLUSION: