Copy_____of 1000 Copies

PRINCIPLES OF TRADECRAFT

Militia Free Press
Post Office Box 47095, Kansas City, Missouri 64188
(A Subsidiary of *The RESISTER*)

PRINCIPLES OF TRADECRAFT

Militia Free Press
Post Office Box 47095, Kansas City, Missouri 64188
(A Subsidiary of *The RESISTER*)

Militia Free Press,
c/o ***The RESISTER***
PO Box 47095
Kansas City, MO 64188

CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

FORWARD

This publication is not intended to be a comprehensive work on the intelligence requirements for resistance, nor on the tradecraft necessary to operate and survive under strict population control measures. It is intended to be an introductory text—a primer that defines organizational requirements and limited operational methodology. Effective resistance begins with knowing what needs to be done.

Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us—the prelude to decision and action by (in our case) underground and resistance policy makers. The underground intelligence organization provides this information in a fashion that helps consumers, either resistance political leaders or militia commanders, to consider alternative options and outcomes. The intelligence process involves the painstaking—generally tedious—collection of facts, their analysis, quick and clear evaluations, production of intelligence assessments, and their timely dissemination to consumers. Above all, the analytical process must be rigorous, timely, and relevant to the underground's policy needs and concerns.

The underground intelligence organization deals with both classified and unclassified information on federal, state and local government, law enforcement and military developments. Its analysts takes raw data and produce finished intelligence by analyzing, evaluating, interpreting, and integrating the various pieces of information. The underground intelligence organization offers the intelligence consumer a broad range of products (which may be presented through a variety of media):

- Daily publications and bulletins or briefings about current developments.
- Biographical reports and psychological studies.
- Assessments, briefs, and memorandums on specific subjects.
- Technical analyses or weapons, weapon systems, and how to defeat them.
- Formal estimates that take more in-depth looks at specific national situations.
- Comprehensive research studies.
- Serial publications and situation reports addressing specialized topics, key locations, or important policy issues.

Some of the best information used in various intelligence products comes from sensitive sources. To protect these sources—whether human or technical—and to ensure the continued availability of the information to the resistance, most intelligence is classified and carefully controlled on a "need -to-know" basis.
There are four categories of intelligence sources, also known as collection disciplines:

1. **Signals intelligence**, also known as SIGINT, includes information derived from intercepted communications and electronic emissions in general.
2. **Imagery**, referred to as IMINT, includes both overhead and ground imagery.
3. **Measurements and signature intelligence**, also known as MASINT, is technically derived intelligence data other than IMINT and SIGINT. The data result in intelligence that locates, identifies, or describes distinctive characteristics of targets.
4. **Human source intelligence**, also known as HUMINT, involves clandestine and covert collection techniques. The following are some of the principal types of collection associated with HUMINT:

- Acquisition of *open-source data* from media, including radio, TV, films, newspapers, journals, and books.
- *Clandestine source acquisition* of information and other data (including photography, documents, and other material) of intelligence value.
- *Data collection.*
- *Debriefing of citizens* of sovereign states who travel or have access to government information.
- *Interrogation* of federal prisoners.

Simply put, intelligence is knowledge, organization, and activity.

Frank Slocum
Intelligence Officer, SF Underground

Chapter 1

INTRODUCTION TO ESPIONAGE

INTELLIGENCE

In order to properly approach the subject of espionage, we must first examine the relationship between espionage and intelligence. We begin by asking a deceptively simple question: what is intelligence?

A Yale history professor named Sherman Kent, who began his intelligence career with the Office of Strategic Services and later served as head of the Central Intelligence Agency's Office of National Estimates, proposed the definition that guides most post-war practitioners. Intelligence, said professor Kent, is knowledge, organization and activity.

Intelligence-as-knowledge consists of three interrelated elements:

1. What is basic, represented by the example of maps, background monographs, or demographic studies.
2. What is current, which briefly stated is the notation of changes or developments in what is basic.
3. What is estimative, which greatly simplified can be called the

informed prediction of changes or developments yet to come.

These three sorts of knowledge are actively required by all nations and apply to common areas of interest: geography, military studies, economics, politics, society, science, technology, and factors that concern the operations of the intelligence function itself.

Intelligence-as-organization is an agency or service which collects and processes raw information, produces finished intelligence, and disseminates this intelligence in response to knowledge requirements set forth by the agency's customers. Such agencies typically consist of broad directorates covering each of several strategic areas and functional divisions, such as "collection," "assessment," "presentation," "support," or "liaison." Published organizational charts should give the reader a general idea how western agencies are run. Those produced by various western agencies provide a view of how we like to think opposition agencies are run.

Bureaucratic distinction tend to color operations and this is no less true for intelligence than any other profession. A significant distinction for us to grasp is the administrative division, made in the United States, between what is overt and what is secret. This posture is adopted in reflex to the U.S. philosophy of intelligence activity; distinctly different from the Russian philosophy, which demands there be no demarcation between overt and secret. All intelligence activity is secret in the Russian view.

Intelligence-as-activity reflects the methods by which intelligence organizations produce knowledge. In theory, the intelligence cycle is one of:

1. Being presented with an informational requirement.
2. Analyzing the requirement to determine the means by which it will be met.
3. Collecting raw information relating to the requirement.
4. Evaluating the information.
5. Translating the evaluated information into statements of probability.
6. Presenting this knowledge to the consumer.

In the United States, as we have said, intelligence activity is divided into what is overt and what is secret. Overt intelligence, which accounts for roughly ninety percent of all finished intelligence, includes the procedure of collecting information from all overtly accessible sources, under circumstances which are in themselves quite harmless. Secret intelligence, on the other hand, is the province of espionage.

ESPIONAGE

What is espionage? Espionage is but one of several means employed to secretly gather raw information. More specifically, the term "espionage" is a legal definition that refers to the unlawful collection and transmission of information. Generally speaking, espionage laws revolve around the concept of unauthorized acquisition of protected or otherwise controlled information, and the subsequent transmission of this information to a third party, usually a foreign power. The question of precisely how the information is obtained is not considered because we assume it will be obtained illegally.

Whether or not espionage is committed in any given instance hinges on three considerations:

1. Who will obtain the desired information?
2. What is the nature of this information?
3. Is communication of the information involved?

We need to consider who will obtain the information because in some countries, mere presence of an unauthorized person is considered *prima facie* evidence of espionage. The presumption is that this individual's presence in a given area or facility will place him in contact with information he is not entitled to receive. An "unauthorized person" is not necessarily just an individual who lacks authority with respect to a certain type of information. A person can be so categorized by virtue of race, nationality, or any one of a number of other reasons.

We introduce the idea of unauthorized acquisition simply because information can be illegally acquired by otherwise authorized persons. A clerk in a code room, for example, can be induced to secretly photograph classified documents. An engineer in a factory can be made to steal critical design drawings. Both of these examples are of authorized persons engaged in espionage.

We are interested in information that is controlled, for the obvious reason that it is not, under normal circumstances, illegal for someone to acquire uncontrolled information.

The matter of communication becomes involved because in most countries, the element of transmission to a foreign power must be present before the activity can be considered actual espionage. Communication of information is in fact pivotal to the legal concept of espionage. Unauthorized acquisition or possession of information are in most cases illegal, but are not considered espionage unless there is evidence of either the intent or fact of communication.

In a manner similar to Professor Kent's portrayal of intelligence, we can define espionage, albeit a trifle artificially, as a legal distinction, collection tool, and craft. We have just examined the legal distinction and will now examine the other two possibilities. We want to bear in mind that the legal distinction indelibly colors

the latter two aspects. It should be obvious that one does not in fact practice espionage unless the appropriate legal conditions are present and one actually breaks, or intends to break, the espionage laws.

Espionage is a highly specialized and narrowly focused collection tool that is only prudently used subject to the following:

1. When there are no alternative means of acquiring the desired information.
2. When available means are inadequate to offer reasonable certainty that the information gained will be accurate, and that the information sought will be the information gained.
3. When the damage from not having the desired information is greater than the potential damage should the espionage operation become known.

Espionage is therefore a tool of last resort. Because of the dangers inherent in any espionage activity, intelligence managers prefer to first exhaust the possibilities of other collection tools. These other tools are known as alternative means; so called because they are an alternative to espionage. Alternative means include the following:

1. Overt collection.
2. Creative reasoning.
3. Diplomacy and liaison.
4. Technical collection.

Overt collection is the procurement of information from freely accessible sources, such as newspapers, public records, broadcasts, or journals, and by direct, open observation of tangible subjects. Overt collection is by far the most successful collection tool, yielding a surprising amount of hard, factual information. Many analysts maintain that fully ninety percent of all finished intelligence may be obtained through overt collection.

Creative reasoning is nothing more than the art an science of informed supposition. It is also the practice of "situation gaming," based upon masses of information subject to controlled analysis and prediction.

Diplomacy and liaison here refers to the solicitation of information from intelligence activities or operations other than one's own, in instances where perceived goals are of a similar or harmonious nature

Technical collection includes the use of satellites, telespectroscopes, infrared devices, air or gas collection and analysis, chemical collection devices, and literally thousands of other technical aids. Code breaking, transmission interception, photography, electronic surveillance, and ordinary broadcast monitoring may all be thought

of as technical collection.

In spite of the above options, there are situations where the only feasible means of information procurement is that of espionage. It is here that espionage acquires its own unique area of responsibility, in service to the following categories of intelligence requirements:

1. Information on opposition organizations.
2. Early warnings.
3. Planning information.
4. Access to denied areas.
5. Piece information.
6. Operational information.

The first category above refers to operations targeted against foreign organizations engaged in intelligence and security functions. Such operations re sometimes referred to as being either "positive" or "negative" in character, and are usually lumped together under the general heading of counterespionage. Positive counterespionage is espionage activity that produces information or fulfills some other purpose such as the feeding of disinformation. Negative counterespionage is espionage activity that provides defensive security, such as the tracking down of enemy agents. Both forms have as their goal the penetration of opposition agencies and the control of opposition agents.

Early warning refers to the acquisition of advanced information relative to the security of the espionage operation's sponsors. In the case of counterterrorism, for example, this might take the form of information that a certain terrorist group contemplates bombing a local bank or other business. To carry this example a bit further, we can also illustrate what is meant by planning information. In this case, the espionage operation meeting the requirement of supplying raw information relative to planning would entail when the bombing is to take place, which bank or business is the target, who will be involved, and what type of explosives are to be employed.

Access to denied areas refers to gaps left in information collected by alternative means in areas hostile to the espionage operation.

Piece information refers to information obtainable through no other means which supplies missing data.

Operational information in information provided by the espionage operation to operations utilizing alternative means of collection. Also included is information bearing a direct relationship to the security of the espionage operation and its continued satisfactory performance.

It is in order to meet the above requirements that the espionage operation is justified. Again we stress that espionage activities are conducted after a careful

assessment of determine whether or not alternative means may be employed to greater success.

The craft aspect of espionage includes all of the methods and procedures employed to secretly gather protected information. In general, such procedures follow a rough pattern which we have summarized as follows:

1. Required information is targeted to a specific location, person, document or other source.
2. A determination of the operational environment is made, inclusive of (but not limited to) these three questions:

    a. What obstacles are to be overcome?
    b. What danger is there in overcoming these obstacles?
    c. Is the information vital enough to warrant risking the danger present in overcoming the obstacles?

3. Routs of access to the target are identified and an optimum route selected on the basis of a target vulnerability analysis.
4. A precise method of collection is selected.
5. Operational security is established and a secure framework for operational command, control, and communication is put in place.
6. Requisite human or other assets are obtained.
7. The target is penetrated and the required information is collected.
8. This information is communicated via secure channels.
9. The operation is terminated.

Craft techniques actually employed in any given operation naturally vary as operational necessities vary. In essence, we may say that the craft of espionage is fundamentally the craft of using human beings as instruments, with or without their knowledge, for the performance of secret activity on behalf of others. In the following pages we will take a close look at how this is accomplished, and how espionage operations are mounted.

Chapter 2

AGENTS

TYPOLOGY

Human beings, when used as instruments for the performance of secret activity on behalf or in lieu of others are known as agents. The doctrine of categorization for agents varies considerably. In an example from early U.S. practice, agents are categorized as follows:

1. *Specialized agents*, recruited for one particular task, or found already in place at targets. Such agents are in the latter event known as "naturals."
2. *Short-range agents*, recruited en masse or individually in large numbers for limited tactical or operational intelligence purposes.
3. *Long-range agents*, recruited on a more selective basis for political intelligence purposes.

These distinctions have now all but disappeared from use. In current practice, agents are categorized as action agents, support agents or management agents.

1. *Action agents* are involved solely with the collection of intelligence information (whether operational, political, or any other sort), and are classified according to their degree of access to the intelligence target:

a. *penetration access*, i.e. "naturals."
b. *surreptitious access*, in which the agent is inserted by means of stealth or subterfuge.
c. *fringe access*, where agents carry out their assigned collection tasks through peripheral contact with the target, target personnel or suppliers, etc.

In general, penetration and surreptitious access action agents collect information by three methods; observation, direct acquisition, and elicitation. Fringe agents are usually limited to the methods of observation and elicitation.

2. *Support agents* are engaged in the performance of general support services, technical support, security functions and communications.

a. *general support agents* include interpreters, collectors of imported materials, those who store materials, safe house keepers, supply and finance agents, training agents, spotters and recruiters.
b. *technical support agents* include forgers, smugglers, electronic specialists, photographers, weapons specialists, camouflage and concealment technicians, and locksmiths.
c. *security support agents* are typically used for countersurveillance, pre-recruitment investigations, as transport agents, and as cut-outs.
d. *communication support agents* include cryptographers, radio operators, couriers, agents who supply accommodation addresses, and those who act as live drops.

3. *Management agents*, sometimes called principals, handle other agents on an individual, net, or cell basis.

SPOTTING

Spotting is the preliminary selection and identification of potential subjects for recruitment. The task of spotting is often performed by support agents specially charged with this responsibility, but may be done by anyone with the knowledge of agent requirements. Spotting begins with a general survey of the operational area and consideration of agent types needed to accomplish the assigned mission.

Principles of Tradecraft

Broadly speaking, agents are selected according to the following criteria:

1. *Access to target*. Access to target is of two varieties:

    a. current access, in which the agent is already present in the target area.
    b. potential access, in which the agent has the potential for inserting himself in the target area.

Access to target is the single most important determining factor.

2. *Environmental requirements*. Environmental requirements include various social, ethnic, and cultural criteria, the agent's age, sex, physical condition, and general appearance.

3. *Personal qualifications*. Personal qualifications include intellect, emotional state, ethics and morals, education, life experience, habits, special talents, long-range usefulness, potential for future use, and degree of attractiveness to the active opposition.

4. Motivational factors. Agent motivation is an extremely important factor. Motivation is generally regarded as being inclusive of one or more of the following elements:

    a. fear
    b. dependency, or desire to please
    c. personal gain, or ego gratification
    d. ideological, or political
    e. vengeance
    f. irrational, or anti-social

Once potential agents are identified from among the target population, they are given a preliminary assessment that is responsive to the various criteria noted above. Additionally, they are assessed in terms of certain contact information, necessary to evaluate the potential agent for security and recruiting purposes. Reporting guidelines for spotters usually follow this simple format:

1. *First contact*. When, where, and how was the potential agent initially spotted? Was contact deliberate or accidental? Who initiated contact: the spotter or the potential agent? Do others know of this meeting?

2. *Follow-ups*. Under what circumstances did any subsequent meetings take place? At what frequency? Was there any seemingly significant time gap between meetings? What were the reasons for these meetings? Were meetings

accidental or arranged? Who arranged these meetings? Were meetings observed?

3. *Nature of relationship*. What relationship does the spotter have with the potential agent? Has there been any perceptible change in the potential agent's attitude since meetings first began? What direction is the relationship taking?

RECRUITMENT

Once spotters have identified a prospective agent and initial assessments are satisfactory, the pre-recruitment development period begins. In some cases development may be handled by the spotter, particularly where there is a pattern of subsequent meetings. More typically, pre-recruitment development is the task of a specialist known as the recruiter. The recruiter's tasks are as follows:

1. He must meet the prospect in a seemingly natural or accidental fashion, calculated to set the prospect at ease.
2. He must build a relationship on the basis of that first meeting.
3. The relationship must eventually develop the prospect to the point where he or she in recruitable.
4. The prospect must be recruited for the espionage assignment, and "handed off" to the principal agent who will eventually run the prospect..

The recruiter begins by leading the prospect to believe there is something beneficial to be gained from a relationship, and that both the relationship and the benefits have nothing to do with the prospect's involvement with the target. This aspect of development is mainly concerned with overcoming initial suspicion and normal interpersonal reticence, and with the discovery of "hooks," or vulnerabilities that can be used as the basis for continuing the developmental process.

Once a relationship is established, the recruiter begins to introduce two new aspects: that of dependency, and an interest in the prospect's involvement with the target.

Once dependency is established, the recruiter's next task is to steer the prospect into feeling that any "favors" the recruiter asks are 1) perfectly natural, and 2) a small thing compared to the continuation of the pleasurable, positive reinforcements. These recognition may take place on any one or several of the prospect's mental levels. Gradually, the prospect is unable to refuse any request the recruiter makes.

When this point is reached the recruiter begins to enlarge on a subtle theme of clandestinity that will have been present during the whole of the relationship. This leads to a culmination where the recruiter asks the prospect to do something trivial, but nonetheless illegal and related to the practice of espionage. The theft of a confidential phone book, so a recruiter masquerading as a salesman can "call on potential customers," is one classic example. The prospect accedes to the request,

performs the petty theft successfully and is made to feel that such performances are both easy and harmless. This practice is sometimes known as expanding the area of conscience.

Agent recruitment can take any one of several forms. The form actually used in any given circumstance is determined by the character of the developmental process. The recruitment just described is a classic *warm recruitment*. A notable variation is the so-called *cold pitch*, which bypasses the development phase and abruptly confronts the prospect with the idea of engaging in secret work.

Coercive recruitment forms the third important variation. Examples of coercive recruitment include those effected by blackmail, drug dependency, or physical violence.

In general, the subjects of recruitment are said to be either witting or unwitting. This distinction is necessary to distinguish between agents who are aware of the true nature of their relationship with the principal and the principal's employers, and those who are not. Among the latter are included those agents who are the subject of false-flag recruitment. An example of false-flag recruitment is a clerk who believes she is furnishing information to the staff investigator for a crusading congressman, when in reality the staff investigator has been co-opted by a hostile opposition agency.

AGENT HANDLING

What practitioners refer to as agent handling is aimed at:

1. Rendering the agent amenable to strict control and instilling a sense of discipline.
2. Inculcating proper security awareness and assisting the agent with any cover necessities.
3. Establishing secure lines of communication
4. Directing the agent's collection activities.
5. Providing the agent continuing incentives and motivation.
6. Performing certain limited forms of training, such as the operation of special equipment or the practice of countersurveillance.
7. Performing certain administrative function such as collecting information on the agent and the operation for contact reports, and general housekeeping chores such as finance and general support.
8. Offering a continual reassessment of the agent and the operation.
9. Preparing for agent termination.*

*NB: Greasy spy novels notwithstanding, this simply means the termination of the agent's services. This will either be without prejudice (friendly), or with prejudice (hostile).

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 3

AGENT ORGANIZATION AND MANAGEMENT

PERSONNEL

After agents have been assessed, selected, developed and recruited, they must be organized for maximum operational utility. Agent organizations are managed by career intelligence officers known as case officers or operations officers, who are attached to intelligence stations.

The first task of organization is to locate a secure base from which to conduct operations. Such bases are of two general types:

1. *Legal* bases, operating under official cover, within embassies, consulates, etc.
2. *Illegal* bases, operating clandestinely under non official cover.

Overseas intelligence stations command top priority at diplomatic facilities. Except in rare cases, it is for this reason that bases are usually of the illegal variety.

Bases must be located in facilities affording certain characteristics. Among these are accessibility, natural cover, both for the facility and the visitors, and camouflage. A base located in a dentist's office, for example, would offer a plausible explanation for: 1) repeated visits at regular intervals, 2) special individual meetings, under the guise of "emergency referrals," 3) the possession of certain types of equipment and supplies, such as photographic darkroom, drugs, supplies suitable for flaps and seals work, secure records containers, etc., and 4) could thus serve to camouflage the comings and goings of a wide variety of personnel. Such a base would, however, only be accessible during a dentist's normal working hours.

Bases are established in accordance with the so-called third area rule. The third area rule maintains that bases must be located in areas having little or no relationship to the target area.

Agent organizations fundamentally consist of three elements: the resident agent, principal agent, and action agent. The characteristics of each sort as they relate to the organization are as follows:

1. *Residents*. In order to establish and maintain bases operations officers employ resident agents. Residents are "middle managers" who link operations officers with agent organizations. They are witting of their connection with the intelligence service and often enjoy long-term contractual arrangements. The get their name because they reside in the area from which the operation is mounted; as distinct from operations officers who merely pull a tour of duty in the area. One resident will usually work for several operations officers during his career.
2. *Principals*. Residents employ principal agents in the target area to maintain supervisory contact with support and action agents.
3. *Agents*. Action agents operate at "the end of the line" in contact with the target

Lines of communication between operations officers, residents, principals and agents are not direct. Each of these represent what is sometimes called a station (not to be confused with the intelligence service's field station), where information stops on its way from the target to the consumer. Between each of these stations are support agents known as cut-outs, who provide the organization with its basic security. Cut-outs are known only by sight, and operate as couriers between agents, principals, and residents. Cut-outs are not the only means of securing links. This function is also fulfilled by means of drops, which we will discuss in greater detail elsewhere in this text.

A sample agent organization will begin with the action agent who contacts the target, and passes information to a cut-out or drop. From there, information passes to the principal, who sends material via a similar link to the resident. The resident, in turn, forwards information along to the operations officer, again by secure means.

STRUCTURES

Agent organizations are of two basic types:

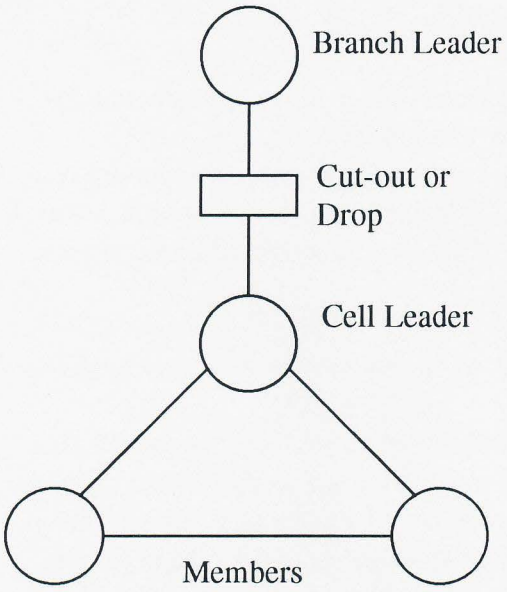
1. *Linear*, in which one operations officer runs one resident who runs one principal who runs one action agent, contacting one target.
2. *Cellular*, in which one operations officer runs one or more residents who run several principals. Each of the principals run several agents, arrayed in cells, offering multiple coverage of single targets, or coverage of multiple targets of related interest.

Cellular organizations can also be linked, in which case they are known as series cells.

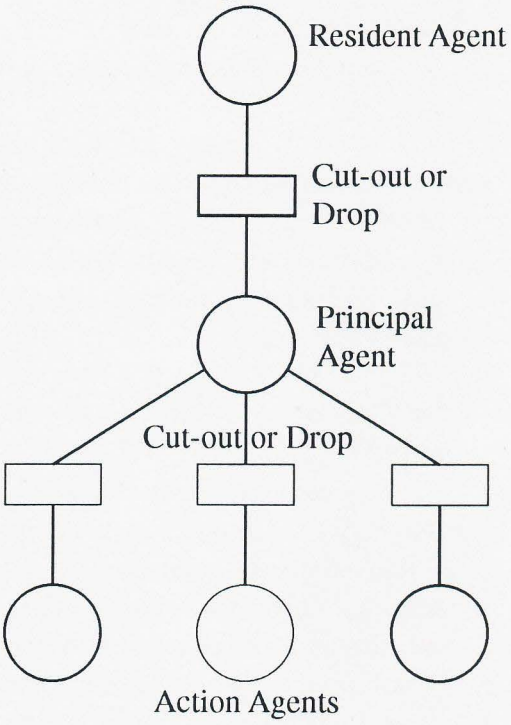
Inter-cell communications links will usually be secured by means of a cut-out mechanism. Although agents in each cell may be known to each other, agents from one cell do not communicate directly with those from another. This forms a fundamental difference between series cells and so-called networks. In networks, agents contact with each other directly and the compromise of one agent thus contaminates the entire network. Network organization is the least secure type of agent organization and is rarely if ever practiced in intelligence operations. Networks are generally reserved for the armed organization of a resistance movement.

Both linear and cellular organizations can be operated either singly or in parallel. Single circuits represent a single contact with a single target. Parallel circuits are simply duplicated organizations set up to verify information and reliability of sources. Parallel circuits offer the possibility of a back-up should the primary circuit be destroyed or otherwise rendered ineffective.

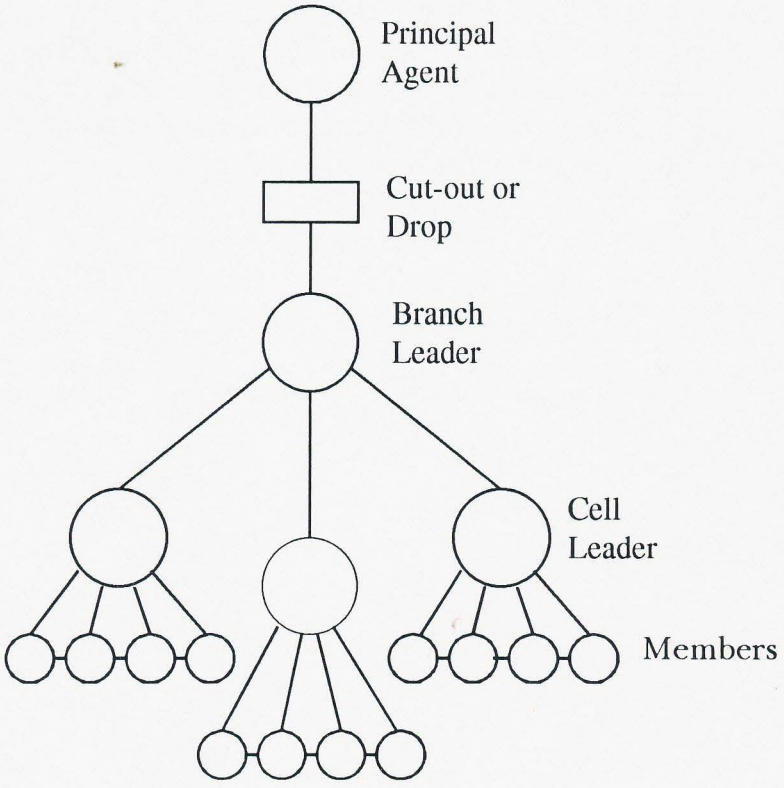
Operational Cell



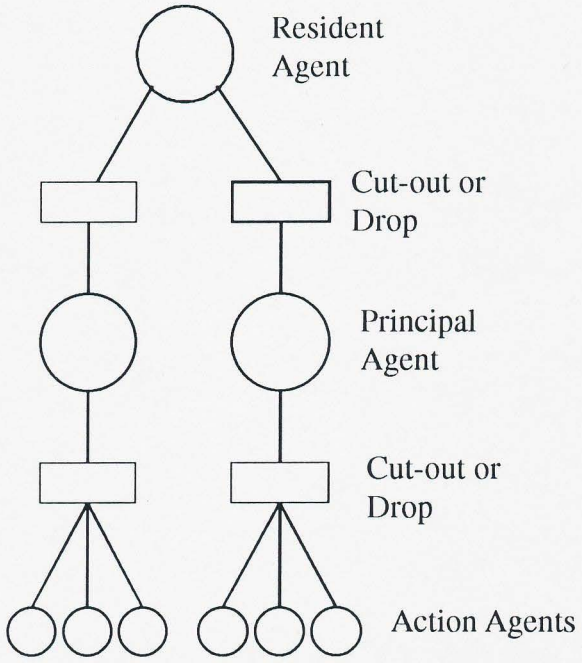
Intelligence Cell



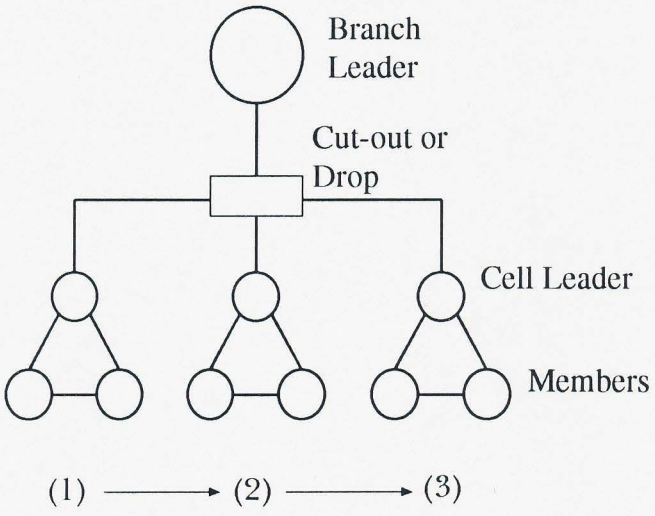
Auxilliary Cell



Cells in Parallel



Cells in Series



THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 4

COUNTERESPIONAGE

CONTROL ELEMENT METHODS

Counterespionage is clandestine activity expressed in either one of two ways: defensively, or offensively.

The defensive aspect is often referred to as the security function. The security function involves physical an investigative measures designed to safeguard information, installations, personnel and operations. The offensive aspect refers to application of active countermeasures, as necessity may dictate.

Offensively expressed counterespionage activity is composed of two elements:

1. The control element, sometimes called preventative counterespionage.
2. The operational element, sometimes called detective counterespionage.

Control measures are regulatory in character and involve the exercise of

influence in five areas:

1. *Control of Identity*. The exploitation of identification systems such as vital statistics certificates, driving and other licenses, etc.
2. *Control of movement*. Limitation or other regulation of internal and external travel.
3. *Control of action*. Use of regulations prohibiting certain activities such as public meetings or possession of firearms.
4. *Control of communications*. Regulation or exploitation of broadcast communications and telecommunications, whether public or private.
5. *Control of publications*. Censorship, tacit or expressed, or newspapers or private publishing.

OPERATIONAL ELEMENT METHODS

Operational measures are uniformly based on the extensive use of carefully cultivated informant services. Operational measures are as follows:

1. *Surveillance*. Surveillance involves the selective use of static observation posts located in the area of targets on continuing counterespionage interest. Examples are foreign consulates, airline terminals, bus stations, hotels, and the homes of suspects. Also included is mobile surveillance of counterespionage targets and sub-targets.
2. *Interception*. The techniques of interception are applied against communications. Included are postal monitors, telephonic and telegraphic monitors, detection and monitoring of clandestine transmitters, and the direct interdiction of secured information systems, carriers, or repositories.
3. *Provocation*. Provocation involves offers of service or supply, the use of false information, incitement, and entrapment.
4. *Penetration*. Penetration of groups or conspiracies may be accomplished by direct involvement, indirect enlistment, or the exploitation of double agents.
5. *Interrogation*. Interrogation is used against targets and sub-targets in custody, and persons named in previous interrogations.
6. *Searches*. Searches are conducted against persons, places, or conveyances. Searches run the gamut from extensive cordon operations to snap searches.

We must also mention the so-called human factors approach to counterespionage operations. Human factors operations involve the production of estimative intelligence intended to portray the psychological profile of a given counterespionage target.

Examples of techniques employed include 1) indirect personality assessment, 2) analysis of written materials by means of word count and frequency of use, 3) indirect monitoring of certain biological functions, 4) observance of historical behavioral trends, and 5) methods seemingly mystical in nature, such as handwriting analysis and astrological charting.

The human factors approach as a "scientific" enterprise dates from World War II, and has been used with considerable frequency in a wide variety of applications ranging from study of Adolph Hitler to the capture of extortion bombing suspects.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 5

COVER

ESSENTIAL ELEMENTS

The term "cover" refers to apparently innocent activity or biographical characteristics designed to protect personnel and admit access to targets. Such activities or characteristics are generated in response to operational objectives of security and performance of the assigned mission. The are supported in varying degree, according to necessity, by a wide range of methods involving manipulation of social structures and relationships, and documentary or other physical evidenced. Deceptively simple in theory, in practice the building and maintenance of cover is a most complex art.

Cover may be categorized in several ways. Typically, cover is divided into two types: general cover, and particular cover.

General cover is described as innocent life that an agent has led and is leading in order to conceal his subversive life (includes past and present). Particular cover is described as the agent's innocent reason for doing a particular subversive act (includes present only or past only). This latter category is further broken down into cover for status (why) and cover for action (what). To these two categories a

third is sometimes added: cover related to ingress or egress.

In recent usage, general cover is regarded as inclusive of particular cover. The following purposes of cover are given:

1. To give the agent a more or less fictitious, yet clearly defined and coherent personality and life story.
2. To account for the documents in the agent's possession.
3. To explain in a logical and plausible manner the presence of the agent at the scene of operations, the target area, or at one specific locality thereof.
4. To allow the agent the freedom of movement necessary for his mission.
5. To enable the agent to contact that strata of people in the target area with whom his mission is concerned.

TYPOLOGY

Cover flows from perception of operational objectives; in ideal circumstances providing natural access to the target. Operationally specified cover is built on the foundation of what are called essential elements of cover: 1) family background, 2) educational and social background, 3) military career (if any), and 4) occupational background.

Cover reaches into the mind of the opponent, thinks as he would think, and then creates a combination of fact and fancy the opponent is prepared to believe. Cover therefore has two additional categories which refer to the degree of falsity employed. These are natural cover, and artificial cover.

The term "natural" has specific meaning in intelligence work. Naturals are potential agents who are already in a position of access with reference to a given target, and must conceal only their contacts with the directing service or organization, or their interest in subjects outside the normal sphere of life and work. Natural cover involves true names in most instances, authentic documentation, and a normal or legal occupation.

Artificial cover, be contrast, involves fabrication of biographical details and documentation. Natural and artificial cover are sometimes known as "legal" and "illegal" cover, respectively.

Cover applies to organizations as well as individuals, and can employ both in harmony. Such operational cover can be any one of three varieties:

1. Organizational cover.
2. Cover derived from cover organizations.
3. Cover derived from front organizations.

Organizational cover is the cover provided by legitimate organizations. The

participation or membership of agents in such organizations may be with the witting or unwitting support of the organization's leadership, motivated by fear, ignorance, patriotism, or a host of other considerations.

Cover organizations are essentially notional, or false. Such organizations are created solely for the purposes of providing cover. Cover organizations may be staffed by a number of legitimate personnel — there to lend a degree of plausibility — and, of course, will be made to seem as if they perform a legitimate function. Political movements, youth groups, religious groups, publishing firms, educational institutions, labor groups, professional societies, friendship societies, and foundations are all obvious examples.

Front organizations — in contrast to cover organizations which exist primarily to mask involvement — mask not only involvement, but also purpose.

TECHNIQUES

Individual or personal cover is built upon elements of the history, talents, and personality of the operative himself. Two techniques of building personal cover according to this rule are: 1) cover transposition, and 2) lesser crime cover.

Cover transposition involves use of the agent's own experiences, with significant periods rearranged to suit operational necessity. Lesser crime cover, so called to refer to crimes less severe than espionage, involves adopting the legend of a common criminal, such as a poacher or black marketer.

Cover extends to notice of linguistic ability, accent, personal habits, clothing, and personal effects (known as litter, or pocket litter). These are the elements which are used to backstop the general outlines of the operative's legend. One method involves use of so-called secret exhibitions. An operative posing as a photographer, for example, may arrange photographic equipment and chemicals in his luggage or rooms in case of surreptitious search.

Backstopping refers to those means employed to lend credence to elements of cover under examination. An agent may claim to be working for an insurance firm; upon a search of his clothing, business cards are found listing the firm's address and telephone number. Upon calling the number or visiting the address, investigators reach a secretary who confirms that the agent is indeed employed by the firm.

DOCUMENTS

In general, documents must be consistent with the cover story, while the cover story, in turn, must explain the possession of the documents, the reasons why the agent got them and from whom he got them. In the case of team operations, documents will be checked to see that no contradiction arises between team members. In training literature documents are typed and categorized as "everything sustaining a cover." These include:

1. Official documents.

2. Semi-official documents.
3. Private and personal documents.

Documents are further categorized by the legitimacy of their use. Documents may be 1) genuine, 2) genuine, but used by a person other than the rightful owner, 3) genuine, but altered or amended by false entries or exchanges, or 4) false.

False papers, in turn, may be made from genuine blanks, forgeries of genuine blanks, or entirely notional papers.

When we speak of the depth of cover, we refer to its logic, durability, validity, and degrees of elaboration. In recent usage deep cover is narrowly characterized as illegal or artificial. history argues that deep cover can be quite natural.

The depth of cover is a reflection of the degree of support afforded a given operation. Due to always elaborate and costly preparation deep cover operations are applied to long-range objectives. Depth of cover is also a reflection of the degree of operational security. Operational security is defined as that state of safety for intelligence installations, personnel, and activities created by procedures designed to protect secret operations and their products against unintended disclosure and covert operations against attributability.

Study of the nature of operational security therefore materially exposes the interactive nature of cover. Distinctions are often drawn among operational security, physical security, and security of personnel. Yet these disciplines are so intermeshed that a failure in one always jeopardizes the other two.

Chapter 6

SAFE HOUSES

Safe houses are secure locations used for meeting purposes, concealment, recuperation and rest. They may be service maintained, group maintained, individually maintained, or field expedient. Such locations include:

1. Rudimentary shelters
2. Private homes
3. Apartments or flats
4. Temporary rooms
5. Farms
6. Business premises
7. Industrial plants

In each case, the safety and security of such locations are deemed to represent freedom from surveillance and arrest. An agent may, in these instances, speak freely of clandestine matters or engage in clandestine technical functions.

TYPOLOGY

Safe houses are in general divided into four types; Manned or unmanned; secret or assisted.

1. *Unmanned/secret.* The unmanned/secret type of safe house is a shelter, such as a shed, cave, cellar, cabin or hunter's hide which is provisioned as necessary and left unattended until needed.

2. *Unmanned/assisted.* The unmanned/assisted type of safe house is typically a home or apartment maintained by a utility operative who does not reside on the premises. So-called vacation homes and time-share condominiums are ideal choices, as the provide plausible cover for transient use and enable the registered owner to deny any knowledge of clandestine use.

3. *Manned/secret.* A manned/secret type of safe house is a "secret room" or concealment chamber in an ordinary residential dwelling or place of business. The "priest holes" of Jacobite England are an example of this type.

4. *Manned/assisted.* The manned/assisted type of safe house is a home, apartment or other dwelling with residents who actively assist the transient agent, providing security, technical expertise, or a wide range of other services.

CHARACTERISTICS

Management of safe houses is governed by the usual requisites of clandestine behavior. In the case of assisted installations, owners or residents will usually have no overt ties to politically or socially sensitive groups, ideologies,, or activities. There are, however, notable exceptions. Prostitutes, for example, are often employed as safe house keepers. Generally, housekeepers will be conservative in all aspects of behavior and appear as normal members of the community in which they reside.

In some instances support personnel will be selected by virtue of their employment. Farmers, grocery clerks, and restaurant workers, for example, are often able to obtain extra foodstuffs without arousing too much suspicion. This could be a valuable ability in an area experiencing sever rationing during a political crisis or war.

Safe house locations are invariably selected with due consideration to the natural cover they afford. Transient hotels or rooming houses, where not subject to controls, are sometimes used. Extensive modification of safe house structures may be attempted, to provide concealment chambers, escape routes, or photographic darkrooms. Physical security measures will be exploited and can involve the use of closed-circuit monitors, specially hardened doors, and sophisticated anti-intrusion devices.

The physical site of safe houses is a consideration. Some hold that installations must not be too isolated, to prevent the effective use of cordons should the

safe house be taken by storm. In general, locations will be selected which do not encumber security unnecessarily and are consistent with the requirements of cover and expected volume of use. Safe houses are also categorized in times of duration of use, i.e. short stay or long stay, and this is also a major factor in selecting a site.

PRIMING

Safe houses are primed or made ready for use through application of safety and danger signals. For a discussion of the principles of advisory signals and indicators, the reader is directed to the memorandum on drops, elsewhere in this manual.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 7

COUNTERSURVEILLANCE

The techniques of detecting and escaping the varieties of surveillance are known collectively as countersurveillance. In this chapter, we will examine traditional methods of physical countersurveillance, providing a guide to their successful use.

As mentioned, countersurveillance involves both detection and escape. Each of these two categories are, in turn, characterized by the presence or absence of assistance. We therefore describe the four general categories of countersurveillance as follows:

1. Assisted detection.
2. Unassisted detection.
3. Assisted escape.
4. Unassisted escape.

DETECTION

Assisted detection involves the use of convoys, or individuals who follow or

proceed the principal at a distance to observe any surveillance efforts. Convoys may be applied singly or in depth. In the case of high priority situations it is not uncommon to find a dozen or more convoys employed. In cities, such convoys will often operate in the manner of a military-type urban patrol, with assigned fields of view from street-level to roof-tops. They will be deployed on both sides of the street, spaced according to eccentric intervals, ahead and behind the principal. Convoys may be in place along a route hours in advance of an intended operation.

Unassisted detection has two general forms; observation, and ruses and stratagems.

Observation can be direct, or involve the well known method of reflection in store windows, parked cars, or objects. Agents are taught to be especially sensitive to the barely perceptible signs of surveillance: studied casualness, deep interest in minor tasks, similarities of physical appearances, and a host of other nuances. Ordinary street activity has a definite rhythm which even the most experienced surveillant can violate. Taking this a step further, we observe that all locations have individual rhythms. The area around a subway station entrance, for example, will include a few shops where people enter and exit, and a degree of traffic through the station itself. Careful and detailed examination of the area will reveal that it is a composite of activity patterns. People move to and fro, entering and leaving the station and shops. Some loiter; some walk briskly. There is an observable mix of age and racial groups. Time will also reveal "ordinary randomness," such as people who pause to get their bearings, or those who drop packages. Experienced countersurveillants, beyond studying visual incongruities, are alert to changes in these patterns.

Ruses and stratagems are widely diverse. Agents may use bait. Adopting an appropriately conspiratorial air, the agent will hastily scribble a note and then drop it on the street or place it in a refuse bin. He or she will then use reflections to observe if anyone retrieves the note.

Change of pace is another common technique. Agents will randomly alternate between fast and slow movement. This is frequently supported by sudden stops and erratic changes in direction. A particularly good method involves retracing one's course several times in succession.

Actions on public conveyances are often employed. The operative will board a bus, pay the fare, then jump off just as the doors are closing. Subways will be used for "cat and mouse," or taxis will be suddenly hired and discharged. Other methods involve changing conveyances several times along a single route.

The "long walk in the country" is a most effective means of unassisted countersurveillance. Boarding a conveyance in an urban area, the agent will travel to the end of the line. Desolate areas with broad vistas are often selected for this purpose. The agent will walk along stretches of isolated beachfront, or through large fields. After a period of rest, the agent will resume progress toward the desti-

nation using a different route.

ESCAPE

Assisted escape involves the use of decoys. Individuals of similar appearance or wearing similar cloths are substituted for the operative at the point of origin. The operative will wait for surveillance to focus on the decoy, then slip away unnoticed.

Individuals are used to assist in other ways. Guards traveling with agents may create distractions, or directly assault the surveillants. In the case of vehicular surveillance, crash cars are sometimes used to protect the principal's automobile by means of staged accidents.

Six methods of unassisted escape are encountered:

1. *Ruses*. The agent changes appearance or interacts with unwitting civilians.
2. *Distraction*. The principal lights small fires, knocks over objects, or cries for police assistance.
3. *Concealment*. The principal hides from surveillants.
4. *Elusion*. The agent pursues an erratic course in dense traffic.
5. *Filtration*. The principal enters crowded buildings with several exits, and utilizes elevators or fire-stairs to "filter" out surveillants.
6. *Outright flight*. The agent relies on speed to make his escape.

TRAPS

Agents sometimes employ small physical traps to determine if rooms have been searched in their absence. Many of these traps are commonplace:

1. A broken paper match is placed under a door, wedged between the bottom of the door and the floor.
2. A strand of hair is wound between objects likely to be separated, such as door and door-frame, etc.
3. Dust patterns, or patterns created by cigarette ash are noted.
4. The water level in toilet tanks is noted with a chalk mark.
5. Tape is placed on the back of drawers.

MAIL TRAPS

Various means are employed to detect suspected tampering with the agent's ordinary or operational mail. The two basic categories are control letters and mail traps.

Control letters are used for the detection of mail covers. Two principal types are used:

Principles of Tradecraft

1. "Junk" mail and deliberately enticing mail are posted under identical conditions, via the same class of service. The agent notes if both letters arrive at the same time.
2. Mail is posted to the target address and a neighboring address. Again, the agent notes if both arrive at the same time.

Mail traps are used in cases of suspected manipulation of mail in order to read the contents (flaps and seals manipulation).

1. Portions of the envelope's contents are glued to the inside of the envelope.
2. The envelope's contents are wrapped in carbon paper, which will leave distinctive markings on the contents should the flaps be manipulated with opening tools.
3. If "wet opening" methods are suspected, chemical measures are employed:

    a. marks are made using a solution of resorcinol and p-toluidine. Upon exposure to steam these turn from pale red or yellow to permanent black or brown.

    b. tannin and iron are kept separate in dry condition by the adhesive gum on the envelope. If they are steamed, they combine to form a permanent ink.

Chapter 8

AUDIO SURVEILLANCE

All audio surveillance systems have three essential components: the detector, the link, and the responder.

The detector is normally a microphone or induction coil. When it is struck by sound waves, small electric currents, proportionate to the sound, are produced. These small electric currents must be transmitted from the target, and this is the job of the link. The link may be a pair of wires or a radio signal.

The responder will contain an amplifier for building up the small current. It may also contain a radio receiver and possibly a recorder. Regardless of its components, the responder's main job is to build up the small currents generated by the detector and transform them back into audible sound.

Reduced to basics, these are the essentials of audio surveillance, and all audio surveillance systems — no matter how complex — will be so configured. In order to approach this subject correctly, we need to examine each of these three components in detail.

THE DETECTOR

The detector is almost always a microphone. The basic function of all microphones is to convert acoustic energy (sound) into electric energy. In general, acoustic energy strikes a diaphragm, which in turn acts upon a transducer and thereby makes the connection. Nine types of microphones are commonly used in audio surveillance systems:

1. Carbon microphones
2. Crystal microphones
3. Dynamic microphones
4. Contact microphones
5. Spike microphones
6. Suction microphones
7. Tube microphones
8. Shotgun microphones
9. Parabolic microphones

The carbon microphone derives its name from its transducing element, which is composed of carbon granules. It is not a self-generating device, for DC voltage must be applied to the transducing element. This voltage then varies in step with the sound striking the diaphragm. The carbon microphone is a low-fidelity device that responds primarily to voice frequencies. It does have good sensitivity and high output, is extremely rugged, and functions well in both heat and cold. Most telephones, for example, still employ carbon microphones.

Carbon microphones are a low-impedance device, having a nominal impedance of approximately 50 ohms. Impedance is the total resistance of a circuit or electronic device to alternating current. It is extremely important that the impedance of a microphone be matched to the input impedance of the responder. If there is a mis-match, a serious loss of signal will result. Because of this, when a carbon microphone is used, you will usually find an impedance matching transformer also in use to match it to the responder.

The carbon microphone is probably the most universally used detector in audio surveillance. It is a non-inductive device that can be used with ordinary telephone or house wiring.

In contrast to the carbon microphone, the crystal microphone is a high-impedance device. It is a self generating device that requires no external power. The acoustic energy striking the diaphragm causes the crystal element to be squeezed and this generates an electrical current in step with the energy. It is a fragile microphone that will break easily if dropped and is affected by extremes of temperature. It is also susceptible to inductive fields when connected to an unshielded line. Because of this, a shielded wire must be used to connect this microphone to a responder. A shielded wire is a single wire or pair with a woven metal shield to ward off stray

inductive fields.

Crystal microphones have a good frequency response. They are not, however, as sensitive as carbon microphones, not do they have the same high output.

Dynamic microphones are widely employed. Dynamic microphones are also referred to as "moving coil" microphones. The diaphragm is attached to a coil of wire which moves in a magnetic field, thereby generating electrical energy in step with the sound. It is a self-generating device, with an impedance of from very low to about 1,000 ohms. This microphone can be made very small and is commonly employed in miniturizations. It is an inductive device that requires the use of a shielded wire. It is quite sensitive, has excellent frequency response and is reasonably rugged.

Contact microphones are designed to respond to vibration. Fundamentally, contact microphones are crystal microphones that, when placed against a flat surface, will pick up vibrations from the surface and convert them into electrical impulses.

When sound is generated, it causes all surrounding surfaces to vibrate in step, and it is this fact that is exploited by the use of the contact microphone. A contact microphone may be placed against a wall or window to capture sound without entering the target room.

Spike microphones are nothing more than contact microphones with a long spike attached to the sensing element. In use, a small hole is made in one side of the wall and the spike extended through the hole until it contacts the surface of the target wall.

Suction microphones are another application of the contact microphone. A rubber suction cup is used to hold the microphone against the target surface. Wither a crystal or a dynamic microphone may be used with a suction cup.

Tube microphones are usually of the dynamic type. Essentially, it is a microphone with a long plastic tube extending from the hole that admits the sound pressure to the diaphragm. The tube may be rigid or flexible. The purpose of the tube is to enable the microphone to be placed at some distance from the wall of the target area. Only a small hole is required. The tube is placed in this hole and the sound is channeled down the tube to the microphone. The tube microphone is used in areas where wires would be dangerous, and to defeat the use of metal detection equipment.

Shotgun microphones are used to pick up sounds from a distance. Shotgun microphones are made up of a series of long tubes placed over a microphone in order to restrict the pick up of that microphone to a very narrow angle. A powerful amplifier must also be used.

To be effective, shotgun microphones must be very large, sometimes as long as eight to ten feet. They are also very directional. If a target shifts his weight from one foot to another, sound will be lost until the microphone is refocused. All sounds

between the microphone and the target area are also picked up. Shotgun microphones are line-of-sight devices and must have a totally clear area in which to focus.

Parabolic microphones are also designed to pick up sounds from a long distances. Parabolic microphones are made using a large reflecting disc that focuses sounds upon the microphone's diaphragm. Parabolic microphones have many of the same limitations common to shotgun microphones. The disc must be large, the microphone directional, and it will pick up sounds between the disc and the target.

EMPLOYMENT

The small size of surveillance microphones allows them to be concealed in very small places. In addition, the wire that is connected to the microphone may be no thicker than a human hair. "Wires" may also be painted in by using a special conductive paint, and then painted over to match the surrounding surfaces.

The fact that microphones are connected to wires generally limits their use to immovable objects. When an agent plants a microphone, he must consider how much time he has to make the installation, the size of the area to be covered, how he will run the wires to the listening post, and where he will conceal the microphone so that it will not be detected.

Access to the target area is the key to good microphone installations. If the agent has unlimited access, he may even chip out a channel for the microphone wires, re-plaster the channel and re-paint the entire room. If he has limited time, he will take short-cuts. He may conceal the microphone in a heating or ventilation duct, hide it behind a radiator, conceal it behind a picture, or tape it to the back of a bookcase. If he has access to an adjacent area, he may use spike or tube microphones.

If time is sufficient, the agent will conceal microphones in a place designed to defeat countermeasures. As an example, favorite hiding places are electrical wall outlets, behind acoustical tile, and behind metal objects. By placing the microphone behind metal objects, the agent effectively counters the use of a metal detector.

THE LINK

To get the signal from the detector to the responder, a transmission link is needed. This is the second component of an audio surveillance system. This, like the detector, is usually located in the area under surveillance. The normal home, for example, has electric wiring, telephone wiring, bell wiring, and any number of electric or phone lines that are no longer used but have not been removed. Any one of these wires could be used as a link.

Even live electric and telephonic lines can be used as links. A special radio transmitter, called a carrier transmitter, can be attached to live electric lines to carry the signal out. If a telephone has been altered, the telephone lines may be used as a link.

Wire-linked systems are used in those instances where long-term coverage is

required. For short-term operations where the agent has limited access, a small radio transmitter is the preferred link.

The most common link in use today is the miniature radio transmitter. Such transmitters are readily available, easily to install, and one need not be a trained radio technician. Such transmitters are of two types: battery powered, and AC powered.

The AC transmitter is usually built into some fixture such as a lamp. It may be wired behind a wall outlet. The battery-powered transmitter can be hidden anywhere. A main advantage is that it is quick to plant; a disadvantage is that the batteries wear out and have to be replaced.

The primary reason for using radio links is the elimination of the need for wired between the detector and the responder. Since a radio signal must be used, however, there are still two components of the audio surveillance system in the target area. A radio signal is considerably easier to locate with countermeasures equipment than wires buried in a wall.

INSTALLATION AND USE OF RADIO TRANSMITTERS

Surveillance transmitters are of two types: the variable frequency transmitter, and the crystal controlled transmitter.

The variable frequency transmitter usually has one or two RF stages and two or three audio stages. They vary in quality ranging from cheap units "potted" in epoxy to well designed units giving good results.

All variable frequency or uncontrolled oscillator units have one thing in common: they drift. This means they change frequency with any change of ambient temperature. If the receiver used is cheap and does not have automatic frequency control, it is almost impossible to stay tuned in.

If the transmitter has only one transistor in the RF stage it is virtually impossible to use it planted on a person because the oscillator will suffer from a pulling effect. This is due to movement of the antenna and the change in of body capacity. Transmitters of good design use two and frequently three RF stages.

The crystal controlled transmitter is considered the best type for audio surveillance purposes. It is "rock steady" and will vary frequency only a few cycles over long periods of use and large temperature changes. A crystal should give years of service in a properly designed transmitter.

Disadvantages include the larger size needed to package the unit and higher battery drain.

Three other transmitter variations also need to be discussed:

1. Radiant transmitters
2. Carrier transmitters
3. Remotely controlled transmitters

Radiant transmitters are the most common type used by agents. Radiant transmitters radiate a signal into the air that allows the agent to monitor from a distance that varies with the strength of the transmitter and the sensitivity of the receiver. A survey of all major surveillance transmitters reveals that the average radiant transmitter will transmit from one to three city blocks. To gain range, relay transmitters are sometimes used. A relay transmitter is actually another transmitter that receives the weak signal from the target area and automatically retransmits this signal to a more distant point.

A carrier transmitter is one that transmits its signal over telephone or electrical lines. Actually, the line over which the signal is transmitted becomes a giant antenna for the carrier transmitter. Due to this fact, the operating frequency of most of these transmitters is below the broadcast band. Carrier transmitters are usually AC powered. Many of these devices are built into lamps or electrical appliances.

Remote controlled transmitters contain a receiver and a switching mechanism. Upon receipt of the appropriate signal, the transmitter switches on or off. This type is often employed where periodic countermeasures "sweeps" are suspected.

Installation begins with visual surveillance of the target. The agent must try to establish a pattern of movement and habits of target personnel in order to determine the best time to make the installation.

Following visual surveillance, the agent must decide whether to enter the premises for installation, or make a penetration-type installation. Penetration installations are used where entry is not possible. Some common techniques are as follows

1. The transmitter is installed in furniture, lamps or pictures, which are sent to the target as gifts, replacement equipment, etc.
2. Common attics are exploited.
3. Common walls are exploited.
4. Plumbing is exploited, together with heating and ventilation shafts.

If entry is effected the first task is to hide the transmitter where it will not be discovered. Care must also be devoted to the size of hiding place you will require. If your transmitter is being used with a large battery supply, or a fully extended wire antenna, you will of course need sufficient space. In general, the factors affecting transmitter employment are as follows:

1. *Proximity* to the desired conversation. Even though a microphone may be capable of picking up sounds from thirty feet, it cannot discriminate between the desired conversation and the sound in between. The agent will therefore attempt

to place the transmitter close to the center of the area where the target conversation will be held.

2. *Concealment* opportunities. The location of the transmitter will be affected by the availability of a place of concealment that is both close to the target conversation and not subject to easy detection.

3. Basic *transmission* factors. Large masses of metal tend to absorb radio signals. Large masses of metal may also be used to make a transmitter directional. Concealment places in proximity to metal masses such as plumbing or filing cabinets will require higher powered transmitters.

Generally speaking, the best place to install a transmitter is in a couch or large overstuffed chair. The couch is turned over and the nails carefully removed from the bottom cloth cover. The transmitter is taped or stapled to the springs or wooden frame. The antenna is stapled along the frame, staying away from the metal springs as much as possible. The battery pack is laid out in the opposite direction from the antenna to give a dipole antenna system. If possible, the antenna should be broadside to the receiving location. Radiation from the antenna occurs broadside and not from the end.

A microphone buried in furniture may give a muffled sound, and for this reason it is usually wise to plant an accessory microphone as much in the open as possible. Try to place this unit within ten feet of the target conversation.

Some additional suggestions are:

1. Planter boxes, utilizing a tube microphone among the flower stems (in the case of artificial flowers).
2. The headboard of bookcase-type headboards.
3. Behind the bottom drawer of a dresser.
4. Behind the center drawer of a desk, or in the underside of the desk top.
5. In doors, drilling down through the top edge of the door.
6. In the hem of drapes or curtains.

Transmitters are also placed in automobiles. Installation is usually beneath the dash, with the antenna being used for the transmission antenna. Care must be invested to see that the microphone is placed as close as possible to the driver. When the automobile is in motion, there is a very high ambient noise level.

It is possible to tail a car to a limited degree by listening for the signal in the receiver to become strong or weak. The installation of a signal strength meter on the receiver, and a sensing type antenna, will produce good results in about a six block area. For best results, a ten to twenty watt transmitter should be used and two fixed monitoring locations with direction-finding antennas should be used.

THE RESPONDER

The very weak electrical signal that is transmitted to the agent's listening post by the link must be amplified and converted into audible sounds. In wired link systems, such as we have discussed, a simple audio amplifier is all that is required. Most agents, however, desire to record the conversations they intercept, so a recorder with a built-in audio amplifier is used. Voice-operated switches, that turn on the recorder only when sound is actually present, are also employed. These devices conserve tape and allow the equipment to be left unattended for extended periods.

Radio linked systems must pass through a radio receiver before they are fed to the recorder. The radio receiver contains an amplifier that builds up the weak signal. Voice-operated switches are also employed on radio links.

TELEPHONIC SURVEILLANCE

Telephonic surveillance, although not surveillance per se, is closely related to passive audio surveillance. Telephonic surveillance is actually electronic communications interception, employing three basic modes of attack:

1. Direct taps.
2. Inductive taps.
3. By-passes, or "bugs."

Direct taps require an actual physical connection to the telephone line. They may be made anywhere between the telephone instrument and the telephone exchange. The telephone lineman's handset may be used for direct taps. The agent simply locates the target line, clips the handset to the line, and places the handset switch in the monitor position.

Most direct taps use a wire as a link. Radio transmitters can also be employed. Such line transmitters are of two types: those extracting power from the telephone system; those that use external batteries.

Some of these transmit a radio signal down the telephone line, while others radiate the signal. Again, these may be located anywhere between the target instrument and the exchange.

The inductive tap is sometimes referred to as the indirect tap, since no physical connection to the line is required. As mentioned previously, all wires carrying current are surrounded by a magnetic field. If a coil is placed in the field, some of the current will be induced into the coil. An induction coil is therefore placed near the telephone line and the conversation is inductively coupled to the agent's listening equipment. The induction coil may also be attached to the radio transmitter.

A telephone by-pass is an alteration of the circuitry of the telephone so that it acts as a wired microphone even though the handset is in the cradle. These are sometimes known as "hookswitch defeats." They may be countered simply by unplugging the suspected telephone.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 9

SURREPTITIOUS SEARCH

The well-planned surreptitious search has an excellent chance of success. Although there is no rule-of-thumb method that can be applied, careful planning and proper preparation prior to the entry should never be omitted. In brief, the entry must be rehearsed until every member of the entry group thoroughly understands his particular task. Let us first look at the methods considered helpful in planning.

PLANNING

It goes without saying that such a job is not done in any impromptu fashion. It is the climax of weeks of careful planning and preliminary investigation. This preliminary work is accomplished in four stages.

1. *General survey* to decide whether:

    a. To take the owner of the building or superintendent into confidence and ask cooperation; or
    b. Rent space in the building for a hideout and operate

without knowledge of owner or superintendent; or

c. Rent space but also take one man into confidence; or
d. Enter the space without consent of the owner or superin tendent.

2. *Contacts*, with:

a. Owner or superintendent if either is to be taken into confidence.
b. Watchman and other persons who may be on the scene when the job is done, so that all members of the group will recognize these persons.
c. Other persons, such as employed of the office to be entered, in order to ascertain the usual activities of the office personnel.

3. *Plan* of entry:

a. Protective measures prescribe for persons taken into confidence.
b. Obtain or make keys where necessary and feasible.
c. Arrange escape route.

4. *Preliminary entry*: The plan of entry and exit is tested by an actual survey which differs from the final entry only in the omission of any attempt to obtain and photograph the documents.

Preliminary contacts. After the office or building has been designated. The building superintendent should be investigated. His personal characteristics, his loyalty, his ability to keep a secret when intoxicated or sober should be studied. Only after the investigator has been completely satisfied on these points should the superintendent be approached. It may be extremely difficult to persuade the superintendent to cooperate. The first thirty minutes of conversation will be the most difficult, as the agent must sell the idea of the proposed entry without disclosing his true identity or the true purpose of the search. A reasonable excuse must be invented to fit each individual entry.

The impression the agent makes at this time cannot be underestimated, for he must create confidence. The agent must convince the superintendent or owner that his entry is a patriotic duty; that the skilled group who will effect the entry are competent and that there is no risk of discovery. The agent must, by intimation, leave the impression that unless this search is made the superintendent is guilty of

sabotaging national security.

The agent must not forget that the superintendent has everything to lose *if* his cooperation is discovered: he may be faced with a lawsuit, the loss of a tenant; or lose his job and reputation. In nearly every case, there is no reward except the superintendent's satisfaction of helping the agent. The exceptional case is that in which money is used to persuade. But the trouble with cash persuasion is that loyalty cannot be bought.

After the agent is sure the superintendent is on his side, he can be of material assistance in helping to neutralize the other building employees. The agent should know beforehand the number and background of employees likely to be encountered on the night of the search. The superintendent's records will reveal considerable background information; but personal records are not always accurate, and sometimes background investigations may be necessary.

The night logbook of the building will reveal the amount of traffic on the floor of the designated office. This should be reviewed for the past month to determine the night of the least elevator traffic. However, this record is also open to wide error, for frequently the night attendants are careless about logging people in and out of the building. Finally, the time of the watchman's rounds should be noted.

Building security. In preparing for the entry everything should be done to make the operation safe, and if possible, easy. Pass keys should be obtained from the superintendent for the space to be entered and for the building facilities and exits. At least three duplicate keys should be made, and given to various members of the group, so that in the event of interruption, no one will be trapped. A floor plan, which can usually be obtained from the superintendent, should be studied by all members of the searching party. Structural peculiarities, if any, of the building should be noted; particular attention should be given to hallways and stairways which could be used as a means of quick escape.

Preliminary Survey of the Space. The initial entry is made solely for survey purposes. It should be made in complete silence and with extreme caution, even if the superintendent accompanies the agent. This silence must be maintained until the premises have been searched for recording devices and innocent traps. These include threads, strings, scotch tape, paper clips or any small article which, if disturbed, will indicate that the premises have been entered.

Silent recording devices operate automatically, and are equipped with a switch which is so sensitive that it starts recording the moment a word is spoken in the room. The evaluator must be constantly on the alert for these traps, and under no circumstances should he remove an object from a dust-covered surface unless he can replace the dust. Dust may replaced by partially filling a small atomizer with dark powder (talc mixed with powdered charcoal).

After these precautions have been observed, the agent must make a detailed survey of the physical characteristics of the premises. The agent should examine the

windows to ascertain if "black-out" curtains are needed. The number, size, and method of affixing the curtains may have to be considered. Next, the agent makes a sketch (using the floor plan) of the position of the furniture, safes, and files.

The name of the occupant of each office may be obtained through checking the telephone extension numbers with the office switchboard. When a safe is found its name, description, and locking device should be noted. This information will materially help the safe expert with his task as he will need time to study in detail the specific locking device prior to the proposed entry. When possible, lock numbers should be noted so that a key may be made.

Next, a room, apart from the area to be searched, should be selected for the camera equipment. A small cleaning storage room, an electric closet, wash room, or small inner office should be selected for this purpose. In the event of interruption, it requires some minutes to dismantle the camera. When camera space is selected outside the office building being searched, there is always the possibility of returning at a later hour and removing the equipment.

Communication between security men on the outside and the group working within the space must be studied. In some cases the use of the portable radio is not practical and the group may be forced to use a telephone (lobby to space), or a prearranged signal. In one case, a security man on the opposite side of the street from the entrance of the building signaled an interruption by lighting a cigarette which was observed by a security man watching from a window in the building being searched.

Having completed the survey the group must then be selected and trained for their specific tasks.

SELECTING PERSONNEL FOR SEARCHES

Great care must be exercised in the selection of the members of a searching group. Success is only possible through the coordination of every member of the group regardless of the task he must perform. The member who must spend the entire night in a darkened elevator, provided for an emergency exit, is considered just as important as any other member. Below are listed the personnel and their specific duties.

1. *Agent in Charge* who must organize the search and assume full responsibility.
2. A *safe expert* who must open safes by the manipulation method.
3. A *lock expert* who must have the ability to pick any type of lock.
4. A *camera expert* who must be able to produce excellent prints under hazardous working conditions and assemble and dismantle a portable camera in ten minutes.
5. A *flaps and seals* expert who must be able to open any type of

envelope and wax seal to replace same within thirty minutes time. The work must be done so skillfully that envelopes can be examined under UV light and defy detection.

6. An *evaluator* who must be able to run through papers and documents and decide, in a matter of split seconds, what documents and papers must be evaluated.

7. *Security men*, whether used inside or outside of buildings, who must have courage and active minds capable of meeting any emergency.

8. *Radio operators* who must know their equipment, have courage, and who do not lose their heads in the event of an interruption.

EQUIPMENT

Equipment carried by the searching party is listed below. All suitcases, bags, and props should bear stenciled cover names.

1. Portable document camera.
2. Camera replacement kit containing kit containing two extra flood lights, two sections of twenty-foot extension cord, extra lens assembly, and assorted batteries.
3. Ample supply of film.
4. Cover props ("building sway engineers").
5. Individual cover identification cards.
6. Bag containing an ample supply of flashlights and sufficient extra batteries to last six hours. The three cell flashlight is superior to a blackjack in an emergency.
7. Portable UV kit to examine questioned letters and documents.
8. Kit containing set of "black-out" curtains.
9. Flaps and seals kit, complete.
10. Emergency interruption kit containing several lengths of rope, adhesive tape and gags.

The specific type of entry must be your guide relative to arming your group. Gas guns, pencil type, are useful where care must be exercised in searching offices of important officials.

With the aid of the floor plan and notes taken during the night of the preliminary survey the final plan is discussed and decided by the group. The time of actual entry is set, evaluators are briefed on any available background of the target subject and subject's associates. If portable radios are to be used they must be tested in the area. The camera expert must be carefully check his equipment. Security men must know precisely what is expected in a case of an interruption.

Time of arrival must be set. An inventory of all equipment must be carefully

checked before departure is made in order that no incriminating evidence may be left behind indicating that the office has been searched.

Chapter 10

CONCEALMENT

CONCEPTS

Study of concealment begins with categorical notice of what is to be concealed and how concealment is to be achieved. These tow primary factors must be examined through the organizing mediums of a conceptual framework, and a discussion of technical means.

Conceptual framework. Concealment is a three-fold process of manipulation involving 1) the objective; 2) the observation or detection process, inclusive of the observer; 3) the operational environment.

The objective of concealment is both general and specific. According to the Oxford English Dictionary, the verb "conceal" means, "...to keep from the knowledge or observation of others." Thus, the broad objective of concealment is to hide. The specific objectives of concealment are determined by what one desires to be hidden. They also serve as the causative factor of the observation process. Specific objectives fall into one or all of three categories:

1. *Concealment of matter*. This category includes human beings,

artifacts, objects, material substances; all things having dimension and form.

2. *Concealment of activity*. This category is self-explanatory. In the sense that concealment is activity this category includes concealment of concealment.

3. *Concealment of information*. Includes concealment of intention, knowledge, belief, any information expressed verbally or non-verbally.

The *observation* process is founded in:

1. Perception, whether sensory or extrasensory, human or artificial, assisted or unassisted.
2. A point of reference to which perception is compared.
3. A point of reference to which comparison is reported.

The manner in which artificial perception is constructed tells us a great deal about the mechanics of human perception. Artificial perception, such as that produced chemically, electronically or by any other means, is composed of samplings arrayed in comparison against a postulated norm. The operator of artificial perception devices noted the character of these comparisons and arrives at judgments based on the presence or absence of similarity to the norm. So it is with human perception. Human perception is arrayed in fields: visual, audible, tactile, gustible, and olfactory. These fields sample stimuli, samples are normatively compared, and judgments are reached on the basis of comparison.

For the immediate, somewhat limited purposes of this study, we will consider operational environment in terms of two postulates:

1. An environment in which the operator is subject to active observation, i.e. search.
2. An environment in which the operator is not subject to search.

SEARCH METHODS

Before discussing various search methods, we need to briefly consider what it is the operator is most likely to conceal:

1. The operator must conceal himself, in the sense that his cover dictates, and if necessary adopt various disguises enabling him to live his cover.
2. The operator must conceal clandestine equipment.
3. The operator must conceal supplies introduced from outside the target area, such as arms, explosives, etc.
4. The operator must conceal both the fact and substance of clan-

destine communications with his principal.

In general, these objectives can be reduced to two categories: 1) *structural concealments*, in which premises or locations are subject to search; 2) *personal concealments*, in which individuals are subject to search.

These two categories naturally produce two corresponding categories of searches; the structural search, and the personal search.

Structural searches are undertaken with the object of locating individuals and controlled objects or materials. Such searches may be routine, as in the case of random "snap searches," or controlled border points; or they may be special, based on tips or suspicions. They may be conducted in the operator's presence to affect arrest, or his absence to collect evidence. They may be obvious, or surreptitious.

Searchers will make detailed advance preparations for special searches in order to fully exploit the element of surprise. Such preparations are inclusive of:

1. *Reconnaissance*, designed to discover plan of the location, lay out of rooms, exits, possible concealment chambers, approaches, ground surfaces, walls, trees, flowers, shrubs, garages, attached buildings, telephone service, electrical service, etc.
2. *Investigation of occupants*, to discover habits, possible informants, watch-dogs, etc.

The approach of searchers will usually be unobserved and very sudden. A cordon will be placed around the location and there will be a simultaneous penetration of all possible entrances. This will be accomplished with considerable speed. Individuals present will be rapidly collected in one room, and thereafter any "wanted" individuals will be taken individually to their own room or other quarters in order to establish ownership of various articles. Generally speaking, there will be two or more searchers for each individual at the target location.

Protection against search is a function of concealment. Effective concealment may defeat routine search but it is ineffective against special searches. If possible, no incriminating persons or objects should be kept at sensitive locations. The operator must practice orderliness, so possible surreptitious searches will not go unnoticed. Informants should be cultivated from among potential searches to warn of impending raids. A signal system should be devised for warning visitors when a safe house or other location is under search.

Emergency concealment aids must be present at every safe house. Individuals may be concealed on or under the roof, in chimney stacks or cistern tanks, inside wardrobes, cloths baskets or dustbins, between ceilings and floors, under stairs, in false tops above cupboards, in lofts, or in hides. Documents may be concealed behind pictures, under tables and beneath carpets, in fireplaces, hollow beams, holes

bored in door traps, in furniture, in windows, behind skirting and picture rails. Weapons may be concealed under refuse heaps, in water tight cases in tanks and wells, behind loose bricks or in piping.

Some operators, particularly couriers, are sometimes forced to carry documents or incriminating objects on their person. The active opposition is aware of this, and as noted in the chapter on counterespionage methods, uses personal searches as an active countermeasure.

As in the case of structural searches, personal searches be routine or special. In general, routine searches may be defeated but special searches, which sometimes last up to 48 hours or more, are never defeated.

Searchers will try to capture the suspect unaware, either by sudden arrest or by detaining ostensibly on "routine" business. The subject will be closely supervised immediately before the search. After capture, no smoking, eating or drinking will be allowed and the subject will be isolated (under observation) to prevent his "planting" incriminating evidence on a third person. The subject's immediate environment will be examined to determine if he has left behind any case, umbrella, overcoat, newspaper, etc.

Usually, an observer will stand by to note any expressions of distress or relief on the subject's face as the searchers proceed with their task. Interrogation will not generally be conducted, but seemingly innocent conversation will be employed to trap the subject. Al personal effects will be searched separately, and the search will be methodical, proceeding from the clothing to the body.

Protection against search. Avoid carrying incriminating objects whenever possible. If selected for search at a control point, do not assume the worst. This search may be a routine "frisk." Effectiveness of the search depends on the human element, e.g., a low-ranking searcher who is hesitant to take responsibility for ruining cloths, a searcher who becomes violent if assaulted, etc. Try to determine what the specific object of the search is, and the focus attention accordingly so that sensitive items may go unnoticed. Control your reactions and maintain an attitude consistent with your cover. The normal emotion in such instances is bored compliance with traces of respect. Attempt bluffs by simulating consternation at the discovery of innocent articles thus distracting attention.

Emergency concealment aids. Emergency concealment aids intend to assist during personal searches fall into three categories:

1. *Cloths.* Hat bands, linings, collar, tie, shirt (under label), padding in shoulders, lapels, double pockets, seams, buttons, soles and heels of shoes, tags of laces.

2. *Body.* Hair, nose, ears, mouth, stopped teeth, false teeth, false limbs or eyes, finger and toe nails, bandages, navel, body cavities.

3. *Effects.* Glasses, lighted pipes, cigarettes, sticks, umbrellas, split

postcards, candy, gum, envelopes, books, newspapers, hotel labels, camera, soap, talcs.

CONCEALMENT

Earlier we defined concealment as a "...three-fold process of manipulation." This manipulation process itself can be defined as involving:

1. An assumption of a norm.
2. A known category of perception to be defeated.
3. A time frame.

Into these elements are injected any one or all of three variables: Disguise; deception; secrecy.

Each variable serves an element of the manipulation process in consort with each other variable. *Disguise manipulates the object*, *deception manipulates the observation process*, and *secrecy manipulates the environment*.

Reduced to basics, the specific methods of concealment are rather simple:

1. With reference to *disguise*, we find cosmetic changes in appearance, or substantive changes of form.
2. With reference to *deception*, we find the technique of imbedding, or blending, which sedates or redirects attention, and dispersal, which expands attention.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 11

CLANDESTINE MEETINGS

Face-to-face meetings, conducted secretly between operational personal, are known as clandestine meetings. Such meetings are employed with some frequency, principally with regard to administrative and management function.

In general, the advantages of clandestine meetings are: They save time; they are used as a countermeasure against some forms of surveillance; the offer a measure of certainty; they provide a means of exercising control; they are used for training the agent; certain forms of supply can be accomplished in no other way.

The stress and delicacy of clandestine meetings reflect concerns of security. Participants may be under visual surveillance and the link between them may be discovered by direct or indirect betrayal. Accidental observation is also a consideration, as are snap searches. In cases where something physical is being passed, apprehension of the participants will provide direct evidence of the clandestine activity.

TYPOLOGY

Clandestine meetings are divided into four different categories:

1. Meetings between unacquainted operatives.
2. Meetings between acquainted operatives.
3. Meetings between operatives and outsiders.
4. Silent meetings, or brush contacts.

Unacquainted operatives. Meetings between unacquainted operatives require secure prearranged identification signals and special briefing. The general description and distinguishing features of each operative must be established and according to operational necessity known by one or both. The security problems inherent in the meeting must be analyzed. There may be risks in permitting certain operatives the ability to extensively describe others they are to meet. The description must preclude the possibility of accidental recognition of legitimate parties who just happen to be at the meeting site.

1. *Artificial descriptive points*. One approach to the problem of providing descriptions is the use of artificial descriptive points, innocuous enough in themselves, which offer operatives a means of recognition. This technique is sometimes called "showing the flag." Examples, which should not be confused with safety signals, described below, include to timeworn flower in the button hole or uniquely folded newspaper, familiar enough to readers of fiction. Artificial points are often given in lieu of physical descriptions involving height, weight, color of hair or color of eyes. They must be obvious enough to spur recognition, yet common enough not to attract unwarranted notice. These points may also be made to mesh with prearranged dialogue.

2. *Unique objects*. Unique objects, such as consecutively numbered currency or two halves of the same bank note, were one used as a means of identification and this practice was continued professionally as late as World War I. Experience shows, however, that this technique should not be employed due to obvious liability in case of search or arrest.

3. *Prearranged dialogue*. Once initial recognition is achieved, the operatives must approach each other. At this juncture identification is made and a method often employed is that of a prearranged dialogue or "paroles." This is sometimes known as "the secret conversation." For example: assume that the artificial descriptive point is a volume of Shakespeare. One offers: "I have never read Shakespeare." The other replies, "Do you mean William, or some other Shakespeare?" This is the first exchange. First exchanges are sometimes followed for safety's sake by a second exchange unrelated to the first. Such harmless dialogue must be structured to prevent accidental conversations with legitimate characters and must leave no question marks.

Acquainted operatives. Meetings between acquainted operatives obviously do not require prearranged identification signals. In every other respect they do not and should not materially differ from other types.

Operative and outsider. Meetings between operatives and outsiders are in practice avoided but sometimes become necessary. In cases where obvious risks are weighed and found acceptable, such meetings will be attempted subject to extensive security procedures. A classic example taken from World War II is the stranger who approaches a member of the resistance, asking to join an armed band. Is he sincere, or an agent provocateur? In practice, if subsequent meetings are decided upon these will be handled by the operative first approached. The assumption in such cases is that if the stranger is in fact an agent provocateur then the operative first approached is already blown.

Other countermeasures include:

1. Loyalty tests, in which potential group members are subjected to mock capture and interrogation.
2. A sudden summons to meet with security personnel under ominous circumstances, designed to reveal signs of nervousness.
3. "Leaks" purported to inform the recruit that he has been blown and is marked for execution.
4. False meetings arranged for suspect members.

Silent meetings. Silent meetings, sometimes called brush contacts, are arguably not meetings at all. Orthodox silent meetings are conducted according to the rules of clandestine meeting practice and are normally used solely to pass something such as a message, or device. Examples are the exchange of briefcases in an airport, or folded newspapers during a momentary pause on a park bench.

FREQUENCY

Clandestine meetings are further categorized in terms of their frequency: Regular meetings; special meetings; control meetings.

Regular meetings. Regular meetings take place according to a prearranged schedule and frequently involve the same site or sites. Such meeting will also be supported by fallbacks, or alternative meeting times and sites, in case the regular meeting is missed for any reason.

Special meetings. Special meetings take place in response to special signals or requests, typically when the matter is of some urgency. Such meetings may or may not be supported by fallbacks.

Control meetings. Control meetings are functionally a combination of both regular and special and are used in instances where a communication link has been broken or lost. In such cases, the operative must come to a prearranged site at a

prearranged time to re-established contact. Another sort of control meeting involves use of "places of conspiracy." Places of conspiracy are utilized in emergency circumstances when an operative has been isolated through the capture or compromise of his immediate superior. In this case, the operative knows to visit a predetermined site at a particular time of day, showing certain recognition points. A representative of the clandestine group takes note of the time and recognition points, and if these are correct makes the approach.

CLANDESTINE MEETING METHOD

Site selection. Meetings are held in the open, in public places and conveyances, under safe circumstances, and at a variety of other sites.

Sites should be selected on the basis of the ease with which countersurveillance may be practiced. They must be manageable. Deserted areas, for example, are ideal from a countersurveillance point of view, but assuming active opposition, the appearance of one agent in proximity to another in such an area may prove cause for contamination. Granting this, more public places, such as parks, museums, parking lots, and a host of other locations are often used, Such places, unless selected with considerable care, can be unmanageable due to the volume of foot traffic and surrounding vantage points. A worth while practice is the use of pre-surveyed sites where ordinary traffic and activity have been observed over a long period of time.

Sites selected must actually exist, and must be accessible to both parties at the time set for the meeting. If audio surveillance is a factor, the sites should present participants with a measure of safety.

Cover for meeting. Obviously the site and the cover must closely mesh. There must be a plausible cover for every meeting and each operative should be fully aware of the details of this cover.

Request for meeting. In the case of special meetings requests are necessary. These are accomplished in any one of several ways. Distinctive arrangements of objects, chalk marks, and classified advertisements have all been used to signal requests.

Safety signals. If an operative discovers or suspects he is being followed to a meeting site, it becomes incumbent upon him to inform his compatriot of impending danger. To provide for this contingency safety signals evolved. Used in addition to recognition points, safety signals silently advise meeting participants: if it is safe to approach; if surveillance is suspect; if a fallback is feasible.

Arrival and departure. Vigorous, often elaborate and time consuming countersurveillance is practiced by both participants on the way to and from the meeting site. Convoys and other countersurveillants are frequently used to guard participants. Guards are also used in the vicinity of the site itself. Another technique frequently employed is the staggered arrival. Participants arrive separately at inter-

vals, sometimes as long as thirty minutes or more. Each participant has his own signal to use for the following participant.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 12

DROPS

Drops, known variously as "letter drops," or *boites aux lettres* (lit., "letter boxes"), are identified as a person, place, conveyance, or object used to transmit messages, money, or equipment in secrecy between operational personnel. Drops are used in both internal and external clandestine communication.

Advantages. Drops are used in preference to clandestine meetings. In general, the advantages of drops are greater secrecy and greater security.

Use of drops can reduce the number of clandestine meetings and offer considerable flexibility in time. There is no direct contact between parties, and assuming the drop remains inviolate, only one operative is exposed at any given moment. Drops may be established in depth to facilitate increased isolation of either sender or receiver, or used to create a reserve of operational necessities. They are also adaptable for use by different types of personnel, such as low-level utility operatives or those handicapped by poor language skills.

Disadvantages. The principal disadvantage of drops is uncertainty. While loaded, materials in drops are outside the operative's immediate control. Drops are also liable to accidental or deliberate discovery with subsequent adverse manipula-

tion, and the ravages of fire, flood, or wild animals. Extensive use of drops may also have a negative effect on management. Fewer meetings decrease the opportunities to train and evaluate agents.

Uses. Drops are used for both long and short term storage. Long term storage is calculated in days or weeks; short term in hours. When employed for the purposes of communication, drops may hold original documents or full-sized copies; or, alternately, reduced reproductions on film. Film is usually undeveloped, and placed in "trapped" containers. Documents may be in cipher or clear text. As stated above, drops are also used to transmit money or supplies. Examples of the latter include weapons, medical equipment, or other technical apparatus.

TYPOLOGY

Drops are of two principal types: live drops; dead drops.

Live drops. Live drops may be witting or unwitting, i.e., they may or may not operate with knowledge of the clandestine purpose. They are located in stores, restaurants, offices, or small shops such as those maintained by news agents or tobacconists. These locations provide ease of access for couriers and enjoy a high degree of normal, transient foot traffic.

Another form of live drop is the so-called underground mail station. Such drops may be located in safe houses especially developed for the purpose with elaborate concealment chambers. As materials are received, housekeepers send coded signals or messages to the next link of the courier line, advising that service is necessary.

Dead drops. Dead drops are categorized variously by type or location. In the former category we find stationary drops, and portable drops. In the latter category we find urban drops and rural drops. Both categories admit of mobile, or "roving" drops.

Stationary dead drops are selected or prepared in meter boxes, lamp-posts, fences, behind mirrors in washrooms, and a host of other places such as crevices in rocks or clefts in trees. Portable dead drops, also known as "inanimate drops," are discarded or specially constructed objects such as tin cans, boxes, tubes or stones. Magnetic key-boxes, used to hide a duplicate key beneath an automobile bumper, can also be used as portable drops. Mobile drops are located in conveyances, popularly the lavatories on trains, buses, or aircraft.

Urban drops are those located in public or otherwise freely accessible places and are typically used for extremely short term transmittals. Rural drops, as the term implies, are located in parks or the countryside. Rural drops are used for either long or short-term transmittals.

AUXILIARY COMMUNICATIONS

Advisory signals and indicators are used to express:

1. Which particular drop is to be serviced.
2. Safety or danger.
3. A drop is loaded.
4. A drop is unloaded.

In common practice, operatives assigned to service drops will do so in response to signaled requests. This signal will usually indicate which drop is loaded, and be supported by a safety/danger signal. In general, the absence of a safety signal is considered a danger signal. Proceeding to the area of the drop, the operative will practice diligent countersurveillance. If the operative is confident of security the drop will be quickly unloaded. He or she will then make a signal to this effect, supported by another safety/danger signal. Safety/danger signals are always made on return journeys, after countersurveillance has been practiced going to and coming from the drop site.

One source has divided signals into five categories as follows:

1. *Graphic*. Chalk marks expressing numbers, letters, or designs; notices appearing in the classified section of a newspaper, postcards, or telegrams.
2. *Objects*. Any small object, such as a flower-pot, or a window shade. The object may be used independently or tangentially; that is, the object and its position may both hold significance.
3. *Light*. Ordinary flashlights, automobile headlights, or infrared light.
4. *Sound*. Radio transmissions, telephone calls, distinctive rings on door buzzers.
5. *Personal*. Articles of clothing, or objects carried.

This same source notes that certain signals or combinations are used solely in conjunction with specific activities. Graphic and object signals, for example, may be used with dead drops. Light and sound signals with some other activity.

THIS PAGE INTENTIONALLY LEFT BLANK