

**United States Army Alaska Pamphlet 381-1**

**DEPARTMENT OF THE ARMY  
HEADQUARTERS, UNITED STATES ARMY ALASKA  
Fort Richardson, Alaska 99505-5000**

**Foreword**

Army Regulation (AR) 381-12 (Subversion and Espionage Directed Against the U.S. Army (SAEDA)), requires that all United States Army military personnel, civilian employees, dependents, and certain categories of foreign nationals are fully knowledgeable of the methods used by the Foreign Intelligence Service (FIS) to gather information pertaining to United States Army installations, activities, and personnel. In addition, personnel must be aware of their responsibility to report promptly any suspicious incident or an actual approach by an FIS agent. This collection of information, containing pertinent facts and background applicable to the SAEDA program is furnished as a possible assist or information source to Military Intelligence personnel. Periodically this is furnished to commanders to update the facts and background information for inclusion in this pamphlet.

Espionage may be defined in general terms as obtaining, or the attempt to obtain, information relating to the national defense of one country with the intent or reason to believe this data will be used to the injury of that nation or to the advantage of the FIS. The ability displayed by the United States in thwarting the attempts of the FIS will determine, largely, the type of civilization that will exist in tomorrow's world.

The entry of the United States into World War I brought espionage to the front as one of our major problems. For the first time in our nation's history, a foreign aggressor deliberately intended to undermine, through espionage and sabotage, the internal security of the United States. German agents operated successfully in the United States, violating its neutrality, and later attempted to disrupt its war effort. Because statutes in effect were inadequate to cope with this type of menace, Congress passed the Espionage Act in June 1916.

World War II gave added significance to espionage. The United States became engaged with enemies who desired passionately and ruthlessly to destroy the nation. FIS agents were eager to obtain vital secrets regarding our defense by fair or foul means. The confrontations of the Korean Crisis, the Cuban Crisis, as well as Vietnam, Desert Storm, and Bosnia, gave added impetus to the necessity for our Security Awareness Program. Even though the Berlin Wall fell and the Cold War is over, that does not allow us to let down our guard. We must maintain a constant vigilance against the aggressive attitude of the FIS and continually be kept informed and indoctrinated concerning the threat to our security.

Each member of this command is provided with a wallet-sized card containing general guidelines as well as who to contact if approached.



DEPARTMENT OF THE ARMY  
HEADQUARTERS, UNITED STATES ARMY ALASKA  
Fort Richardson, Alaska 99505-5000

United States Army Alaska Pamphlet 381-1

1 August 1998

Military Intelligence

Information Guidance and Assistance on Subversion and Espionage Directed Against  
the United States Army

**Impact on New Manning System.** This pamphlet does not contain information that affects the New Manning System.

**Interim changes.** Interim changes to this pamphlet are not official unless the Director of Information Management authenticates them. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

**Suggested improvements.** This pamphlet's proponent agency is the 500th Military Intelligence Brigade, Alaska Resident Office (B Company, 205th Military Intelligence Battalion). Users are invited to send comments and suggested improvements on Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) directly to IAGPD-MID-ARO.

**Distribution restriction.** This pamphlet contains technical or operational information that is for official Government use only. Distribution is limited to United States Government agencies. Requests from outside the United States Government for release of this pamphlet under the Freedom of Information Act or the Foreign Military Sales Program must be to Commander, United States Army Alaska, 600 Richardson Drive # 3200, 99505-3200, IAGPD-MID-ARO.

Contents

	Page
<b>Chapter 1</b>	
Security—A State of Mind.....	1-1
<b>Chapter 2</b>	
Sample Subversion and Espionage Directed Against the United States Army Memorandum.....	2-1
<b>Chapter 3</b>	
Sample Subversion and Espionage Directed Against the United States Army Briefing (Capsulated)* ....	3-1
<b>Chapter 4</b>	
Sample Subversion and Espionage Directed Against the United States Army Briefing (You—The Target)* .....	4-1
<b>Chapter 5</b>	
Sample Subversion and Espionage Directed Against the United States Army Briefing (Foreign Intelligence Service Exploitation of United States Army Personnel)* .....	5-1
<b>Chapter 6</b>	
Sample SAEDA Briefing (Proof Positive)* .....	6-1

\*This pamphlet supersedes 6th Infantry Division (Light) Pamphlet 381-1, dated 3 November 1987.

**USARAK Pamphlet 381-1**

**Chapter 7**

Sample Subversion and Espionage Directed Against the United States Army Briefing (What Makes A Spy?)\* .....7-1

**Chapter 8**

Sample Terrorist Briefing\* .....8-1

\*These samples are for information only. They do not replace training requirements.

**Appendixes**

A. Recommended Reading ..... A-1  
B. Subversion and Espionage Directed Against the United States Army Films ..... B-1

## Chapter 1 Security—A State of Mind

Security begins as a state of mind. What then is security?

It is the proper and effective safeguarding of a command and its personnel against every conceivable enemy action. Conceivable action includes the direct effort of a saboteur to climb a fence or wall to plant a bomb or start a fire. It includes the similar approach of an FIS agent attempting to steal or otherwise obtain documents that may be beneficial or of some importance. Conceivable action includes the effort of the same saboteur or FIS agent to walk past the gate guard with forged or stolen identification or credentials.

Is there any doubt that security begins as a state of mind? The reasonable person, aware of peril, either imminent or potential, takes reasonable steps to protect themselves against that peril.

The prudent householder closes the windows and locks the doors at night.

The banker, custodian of large sums of money, maintains a heavy vault, elaborate alarm systems, and even armed guards to secure the bank's property and valuables. Additionally, the banker is interested in the past and present conduct of the employees to whom the bank's money is entrusted on a daily basis. As simple good business, he/she will hire only persons with clean records of integrity and honesty, from the janitor to the entry-level clerk. If one of the tellers is reported as becoming a regular visitor at the local race track or the more expensive night spots, the banker should take an immediate interest in the situation as a potential threat to his/her security.

The military commander has all those problems of security—and more. He/she has the routine household effects of his/her command to protect from common prowler as well as the more determined burglar. He/she is, ordinarily, the custodian of other property of great value. The greatest treasure possessed by or under the control of the commander is also the treasure that is urgently, desperately, and constantly being sought by the FIS—information of intelligence value.

It should be unnecessary to restate the value of military information. The loss of vital information has led to the destruction of military commands. Information has been a factor in the winning of wars—and their loss. It can be a factor in determining whether the United States, its people, and Government, as now known, will continue to exist.

The emphasis here is on an appreciation of the peril and the establishment of a state of mind that will permeate the command. It is on making security more than routine compliance with regulations, tedious checking in and out of documents, or the casual pacing of a sentry tour. The State of Alaska represents unique security risks/precautions. This is the only state where all United States Army combat equipment must be tested in before it joins our inventory and reaches the soldier in the field. USARAK and the soldiers supporting it are perhaps more vulnerable to approach because of this fact.

The risk assessment for espionage/terrorism for the last several years has been placed as low for Alaska. That does not mean that it cannot, or does not, happen here. In 1993, a Sergeant Gregory, with the 501st Infantry Battalion, was arrested and convicted of passing 40 pounds of classified information to the Hungarian Intelligence agency. Yes, this was a follow-on investigation from Bad Kreuznach, West Germany, however, the arresting officials believe that Gregory was starting his espionage activities again during the 6 months he was stationed here. Gregory was sentenced to 18 years in Leavenworth.

FIS agents and their sympathizers have penetrated every level of this nation's society and have certainly done as well, if not better, in other nations. Throughout the world, these agents and sympathizers stand ready to serve, with or without pay, as espionage agents gathering the smallest crumbs of information or reaching the most vital of the United States secrets. They stand ready to use any means known to man to subvert the members of a military command, to weaken morale, agitate grievances, destroy loyalty, create confusion, or manufacture an incident to disrupt local relations. They stand ready as saboteurs, many of

## USARAK Pamphlet 381-1

them expertly trained and perfectly disciplined to light fires, cut wires, damage vehicles and equipment, and pour sugar into a gas tank or sand into a gearbox.

Their professional staff of agents and spies is armed with incredibly efficient equipment and unique devices to aid in gathering information. It is a reasonable assumption that FIS agents have the most, if not all electrical, electronic, and scientific devices known to this nation's service. It is an alarming, but still reasonable, assumption that these agents possess devices unknown to the United States. It is known that an FIS agent, equipped with a parabolic microphone as much as 100 meters or more away, can pick up every word of a low-voiced conversation at an open window or door. The agent could be miles away from his/her hidden microphone.

The "bugging" of telephone or telegraph wires has been so perfected that actual contact with the wires or instruments is no longer necessary. The telephoto lens has vastly increased the range of the espionage camera. Infrared and other new, high-tech films have made darkness no longer a protection. Detailed and comprehensive technical knowledge of the various espionage devices and techniques requires intensive and continuous study, which the military commander cannot afford to give because of his/her other duties.

Appropriate Army regulations provide security guidance for the commander and his/her personnel. Because these regulations are written for general application throughout the Army, they cannot be specifically detailed for each person nor can they always be more than a general guide for changing circumstances that may affect the command. The most important of these regulations are:

a. *AR 380-5 (Department of the Army Information Security Program Regulation)*. This regulation furnishes broad guidance in the safeguarding, transmitting, receiving, storing, and disseminating of classified defense information. Generally, if you do not know what to do about a classified document or how to handle it, consult this regulation.

b. *AR 380-150 (Security—Access to and Dissemination of Restricted Data)*. This regulation is written in the same fashion as AR 380-5. It provides guidance for transmitting, receipting, storing, and disseminating classified defense information that has been determined to be "restricted data" by the Atomic Energy Commission. Therefore, if you ever come encounter restricted data or atomic energy information, consult this regulation for guidance.

c. *AR 381-12 (Subversion and Espionage Directed Against the U.S. Army (SAEDA))*. This regulation directs that all military and civilian employees of the Army be indoctrinated in the methods used by the FIS, as well as other subversive elements, to subvert Army personnel. Further, this regulation requires that all military personnel, civilian employees, and their dependents report any incident that comes to their attention that may indicate subversion or espionage to the nearest military intelligence office.

Security regulations do not guarantee protection and they cannot be written to cover all conceivable situations; consequently, basic security principles, common sense, and logical interpretation of the existing regulations will be applied. Indoctrination should be so thorough and to such a degree that individuals charged with a security responsibility automatically discharge their duties with logic and discretion without thinking of the rules as an imposed burden. It is possible to achieve a satisfactory degree of security with a minimum sacrifice in operating efficiency. The protection of defense information is the responsibility of each individual who has knowledge or possession of such information, no matter how it was obtained.

Now, we come to the question that is repeatedly asked, "Is security really necessary?" Most definitely! The United States, along with every other nation in the world, has certain military and diplomatic secrets that must be safeguarded in some way. The Russians safeguard their secrets by restricting large areas from foreign visitation and allowing only the most trusted people to leave these areas. The guarantee of security is usually effected by forcing the traveler to leave some member of his/her immediate family behind as a hostage to ensure proper behavior. The United States does not maintain this type of lock-down nor have a super-police state that goes along with it. We would rather make use of another system of security.

## United States Army Alaska Pamphlet 381-1

Our security system is based on our desire to protect our way of life and on each citizen's personal responsibility; therefore, we must establish and maintain an effective security program that will keep our secrets secure. We must always establish and maintain a security classification on pertinent civilian and military documents that are, or could be, of potential value to the FIS. Most important of all, we must establish a systematic and continuous security indoctrination program that will make military and civilian personnel security conscious.

The FIS plays for keeps and security is our first line of defense. The more we keep the FIS from learning of our military potentials, the less they will be able to exploit our weaknesses in time of armed conflict. Our security cannot be effective until everyone in the Army establishment is familiar with the whys and wherefores of security. The best method to get security requirements across to all our military personnel, and in the end make every individual—both military and civilian—security conscious, is security indoctrination.

Why must we have security? The FIS does not "play ball" our way. They have not won a single country over to communism through free, competitive elections. They get into power any way they can—including rigged elections, subversive activity, slander, and outright military conquest. We must realize that a large part of Communist activity is outside the law. This type of activity generally involves spying, sabotage, espionage, forging passports and other travel documents, perjuring, counterfeiting, and spreading disloyalty through the ranks of the armed forces. Using their legal and illegal tricks, FIS agents are aiming toward the eventual domination of the United States as well as any other nation in the world that does not follow their views.

The basic concept and rule for dissemination of classified information applies to all personnel. A person must not only possess the appropriate security clearance. For him/her to have authorized access to certain information, he/she must also have a definite need-to-know. The need-to-know is summarized simply by saying that to perform the official assigned duties they must have access to this classified information. If they officially require the information, then they have the need-to-know.

We must always keep ourselves aware of some of the causes of security leaks. You cannot prevent a disease until you understand its cause. You cannot cure a disease until you know what the symptoms are, so that you can prevent further infections. When we understand why we talk and write too much, we are halfway to being cured. Now, the man or woman who says, "I'm too smart to give away..." is a fool. The only thing he/she lacks to put himself/herself into the correct biological category is a long pair of ears and a tail. Normally, there are four causes of indiscretion. They are ego, ideology, enthusiasm, and ignorance. The four causes of security leaks merit discussion and analysis because they are apt to influence every one of us, no matter how discreet we may imagine ourselves to be.

a. Ego. Ego is the most common cause of leakage. A large percentage of all indiscretions are the result of it and 90 percent of us are vulnerable to it. Why do we brag? Most of us brag to impress someone. There will always be a tendency to brag when you know more than other people you are with, especially when they themselves are "handing out a line" about the inside information they have. It is admittedly very hard to pretend you know nothing when, in fact, you know a lot. To satisfy ego without giving much away, you may find yourself just hinting at what you know. That is fatal. If something that you have knowledge of is classified, you *must not even hint* at its existence.

b. Ideology. Ideology can be a questionable virtue. We do not mean that being Protestant, Jewish, or Catholic is questionable. We do mean that as a nation we are too ready to trust our fellow man. We believe too implicitly in the security of such national institutions as the United States mail, the telephone and telegraph service, and the key that we turn in the lock. Most of us consider ourselves to be pretty good judges of character and not easily fooled. We forget that for an FIS agent to be successful, he/she must be such a plausible and convincing person that no one suspects him/her, least of all those who pride themselves on being good judges of human character. He/she will look exactly like what he/she isn't—a typical American or a typical European with an honest face.

c. Enthusiasm. Enthusiasm is a common cause of indiscretion. Anyone who is really interested in his/her job finds it hard not to talk and write about it. Your first impulse when your organization has done

## USARAK Pamphlet 381-1

particularly well is to talk about its achievements. As time goes on, it becomes increasingly difficult to keep the news of the events that are important to you under your hat.

d. Ignorance. Ignorance is the cause of a vast number of people giving away vital information simply because they do not know that espionage is only a matter of putting two and two together, of collecting bits and pieces of information from a thousand sources, and then cleverly evaluating them into a complete picture. FIS agents are not all lurking in Washington, District of Columbia (D.C.) or on military installations preparing to kidnap a general and steal vital plans. They are quiet, hard-working investigators who go about using their eyes and ears, picking up a little item here and another one there. A scrap of information picked up by the FIS may, at first, seem to be of little value until another report from some other source continues the story and links it up with something else.

Regarding the hard-working, industrious FIS agent, there is one thing that we must always remember. It makes no difference whether the FIS is in a morning coat and striped pants and doing work on a national level or in overalls working in an ordnance depot as a mechanic. It makes no difference whether it is high-level or low-level; the primary purpose in life is to deprive you of the things you hold dear to your heart.

We have a prime example in Aldrich Ames and his Colombian-born wife, Maria Del Rosario. On 21 February 1994, the Ames's were arrested on espionage charges. Over a 9-year period, Ames provided the Komitet Gosudarstvennoi Bezopasnosti (KGB) and its successor highly classified information as well as the names of United States and Russian agents working for the Central Intelligence Agency (CIA). His information allowed the Russians to close at least 100 intelligence operations and at least 10 allied agents were executed. Ames received upwards of \$2.5 million from his Russian handlers.

Now, in summary and conclusion, let us go back to the military commander. One of the commander's primary responsibilities is evaluation, and periodic reevaluation, of his/her command's security requirements. Available to aid in this evaluation are the technical knowledge and training of the security officer; as well as the advice and assistance of Army Intelligence and the Provost Marshal.

Based on the evaluation of the imminent potential perils, the commander must not only install the necessary protective equipment and institute the necessary security procedures. He/she must also establish throughout the command's personnel the state of mind that will implement effective security. With all this reliance upon regulations, operating procedures, manuals, and technical assistance, the commander must place his/her final security reliance upon a state of mind—his/hers and that developed within the command. Command awareness necessary for effective security can be best achieved by continuing study and indoctrination and by strict adherence to those measures prescribed for electronic document, personnel, and communication security.

Does your present state of mind contribute to the security of your organization?

## Chapter 2

### Sample Subversion and Espionage Directed Against the United States Army Memorandum

MEMORANDUM FOR All Personnel

SUBJECT: Subversion and Espionage Directed Against the United States Army (SAEDA)

1. Safeguarding classified information is our responsibility to the military community and our country, and requires the alert and vigorous application of security principles. As military and civilian members, or their dependents, of United States Army Alaska (USARAK), we must be cognizant of the ever-present danger of subversion, espionage, and other acts the FIS may use to threaten our existence as a free and democratic country. In this respect, your support in maintaining our security against the FIS is earnestly solicited.
2. Attempts to procure defense information from each of us are continuous projects of the FIS. Their methods are subtle and varied, so we must be suspicious and cautious in dealing with strangers or persons who are inquisitive about military information. Be alert whenever someone with a known or suspected dissident, radical, or subversive background attempts to cultivate your friendship. Avoid discussions about your job or your sponsor's job in public places, especially when it is a sensitive job. Certain groups, places of entertainment, relaxation, and/or refreshment have, in some instances, been established solely to exploit human weaknesses and gullibility. Do not forget that there are no physical limits within which potential threats may exist. The threat can be a member of a unit; a vocal, nationwide group; a so-called friend or associate; or an innocent-appearing establishment in a city such as Anchorage, Alaska. While on travel status, be extra careful with the helpful stranger who has been so kind in assisting you. Remember that the FIS is always on the job.
3. Every member of the military community has the responsibility to immediately report any incidents or situations that could jeopardize the security of our nation or the military installation. Report the information to the Alaska Resident Office at 384-1622, or 172d Military Intelligence (at Fort Wainwright) at 353-9423. If in a foreign travel status, contact the nearest United States Military attaché, embassy, or consulate. Any information you furnish will be held in strict confidence.
4. Do not discuss the situation or take any action to exploit, apprehend, restrict, or stimulate further pursuance of the matter without proper guidance. In other words, do not attempt to conduct any investigation on your own. Our opposition is intelligent, unscrupulous, and ruthless; and you may endanger your life by your actions.
5. All the security agencies of our nation are working diligently to help maintain the security of our country. Do not delay reporting the information, even though you might believe that it is incomplete or you are in doubt as to the validity of the information. Remember that your alertness and conscientious effort to report this information will make a vital contribution to the security of the United States and this command. Get personally involved in maintaining the security of your country.



### Chapter 3

#### Sample Subversion and Espionage Directed Against the United States Army Briefing (Capsulated)

Our subject today is SAEDA. Since 1958, it has been a requirement that all military and civilian employees be made aware of their responsibility to report promptly any incident of suspected or actual approach by the Foreign Intelligence Service, or FIS.

One of the objectives of the SAEDA program is to make United States Army personnel aware of the threat posed by the FIS. You may ask, "Why is such a program necessary?" It has been determined that too few people, both in and out of the military establishment, recognize espionage and subversion attempts as such.

One of the purposes of an orientation of this nature is to familiarize you with the methods used; to help you recognize the techniques of an FIS agent; to prove to you without a doubt that none of us in the military service, working for the service, or our family members are exempt. You are also here to learn what you should do if you are approached and asked to provide information; or if you have any reason to believe that you may have been selected as a target for espionage; or that someone you know has been targeted. In short, you are reminded that foreign espionage is much more than an entertainment theme on television or in books and movies. It is a continuing threat to our individual and collective security. This discussion is designed to acquaint you with that threat, enable you to recognize it in practice, and ensure that you know how to report any evidence of it you may encounter.

FIS agencies conduct espionage by two methods, one of which is legal or overt, the other illegal or clandestine. The first method involves observation, perusal of publications, and overt activities conducted by military, diplomatic, and cultural attachés accredited to the country in question. The clandestine method involves the covert or illegal activities of trained agents working under some kind of cover to conceal their actual intent and purpose.

One of the basic principles of intelligence collection is to use clandestine methods to collect only that information that can not be obtained through overt sources.

There is information that is not available to the FIS through overt or legal means. As a result, they have to resort to illegal methods. Each of us, whether we realize it or not, has some information that the FIS agent seeks. It may be classified reports or figures or it may be information that has no classification at all and that may seem unimportant. Do not, even for a moment, think it is unimportant! We all are possible FIS targets.

Now, let's look at the main method used by the FIS to collect information in a clandestine of illegal manner.

The FIS places an agent into direct contact with person(s) having access to the targeted information. This is the method that has been most successful and the one for which you must be continually on the alert. They normally approach the individual in such a subtle manner that it is not until he/she is well hooked that the "light dawns." If you are thinking that you would be contacted by someone with a heavy foreign accent, or someone that is known to be a subversive, you are exactly the type of person to whom this lecture is aimed. Please be assured that FIS agents are professionals in the "game" of espionage. Their agents are carefully chosen and extremely well trained. Their methods are calculated; they are patient and content to spend years developing and grooming a target until they deem the time is right to make an approach. Some of these methods may include subverting or blackmailing a person who has direct access to the desired information, exploiting character weaknesses of individuals who may or may not have direct access (but may know individuals with direct access), or audio surveillance.

The cheerful, naive, disarming, and thoroughly American-type who seeks to cultivate you and later ask for bits of apparently unimportant and unclassified information could be an FIS agent. How many recall the cases of James Hall or John Walker? You may not believe this, but both cases began with unclassified information being requested.

## USARAK Pamphlet 381-1

In attempting to recruit a source, the FIS agent has three possibilities going for him/her:

- a. Ideology.
- b. Money.
- c. Coercion, intimidation, blackmail.

Although ideology has been rarely successful in the past, we cannot completely disregard it. Money and blackmail are the methods that have provided the FIS agent with the largest measure of success in the past.

The "setting up" of a person for recruitment through coercion is a "two-way" street. The person can be asked for the bit of "unimportant" information for which the person will be rewarded by a return favor or small gifts. Later, a larger request follows for which the person is offered pay and requested to sign a receipt, or, if the person declines, he/she is told that he/she has already provided information to a foreign power and that if he/she refuses to cooperate he/she will be exposed. The other side of the street is the one in which the "favors" come first, then the request for a "return favor" or the threat of exposure is made.

Now, what should you report?

- a. Report attempts by individuals or organizations unknown to you when they try to gain military information from you.
- b. Report anyone who attempts to undermine or exploit such personal weaknesses as excessive drinking, indebtedness, sexual misconduct, or anything that could cause embarrassment.
- c. Report all attempts or threats to expose past or present misdeeds. Remember, a fine prospect of FIS agents is the individual having that personal secret: "a skeleton in the closet."
- d. Report any attempts of coercion. This type of approach is usually used against an unwilling person who has no embarrassing personal secrets to hide. These are usually threats of harm to relatives who are living in foreign countries. Personnel born in, or who have lived extensively in criteria countries, are vulnerable to this vicious type of attack. They are pressured to give money, information, and other forms of assistance by threats of harm to the unfortunate relatives.

Now, to whom do you report?

- a. You should report it to the nearest United States Army Counterintelligence Office or your security manager. The nearest counterintelligence office on Fort Richardson is the Alaska Resident Office, Building 1 (basement), 384-1622 or 172nd Military Intelligence (at Fort Wainwright) at 353-9423.
- b. You must take no action to exploit or stimulate further contact. Should further contact be necessary, guidance will be provided by the appropriate intelligence agency. The sensitivity of an espionage approach cannot be overemphasized. It is important that you do not discuss the approach with anyone who does not have a need to know.

The methods I have described are not new. Gathering and studying publications, developing and recruiting individuals, and collecting information from careless people have been used in the past, are being used now, and will be used again in the future. The sophisticated techniques of espionage in our time have, however, kept pace with scientific advancements.

Your awareness and cooperation in the vital SAEDA program are absolutely essential. With your assistance, we can minimize the success of FIS efforts within the United States Army.

## Chapter 4 Sample Subversion and Espionage Directed Against the United States Army Briefing (You—the Target)

An Army sergeant, assigned to a sensitive installation in the Washington, D.C. area, was sitting in a cafe near his installation having a few beers. He had just finished bowling and was in high spirits because he had bowled two games well-over 200 and his team won three games. He soon became engaged in a conversation with a middle-aged gentleman who identified himself as Joe. The sergeant soon was telling Joe about the "hot streak" his bowling team was having; that the league was made up of personnel assigned to his unit; the location of his unit; and inferring that the duties he was assigned to were classified because he told Joe he couldn't talk about them. After consuming several more beers, which Joe paid for, the sergeant asked Joe what he did for a living. Joe replied that he was not an American; that he was a member of a foreign embassy located on 16th Street in Washington, D.C. He told the sergeant that he had been in the United States for only 3 months. The sergeant praised Joe's knowledge and use of the English language and told him that he noticed only a very slight accent. The conversation continued and eventually included how much a sergeant in the United States Army earns, his standard of living, etc. The sergeant, proud of the modest home he had bought the previous year, soon was telling Joe about it. In his enthusiasm to show Joe how well Americans lived, he invited Joe to his home. Joe displayed amazement after a short tour of the sergeant's home. He asked how it was possible for a sergeant to own such a luxurious home with so many appliances, such as a washer and dryer. The sergeant's wife replied that it was not always easy, but somehow they managed. After having another drink, Joe departed. In the ensuing weeks, Joe and the sergeant met occasionally at the cafe. Joe always managed to pay for the beer and, on one instance, presented the sergeant with a rather expensive gift for his wife. He explained he had enjoyed her hospitality that one evening and the gift was his only means of reciprocating. One evening, the sergeant told Joe that he probably would not be seeing much of him for a while. The sergeant explained that he had incurred some debts and that there would be little money left for an occasional beer. Of course, you can guess what happened next. Joe told the sergeant that he was interested in certain activities at the installation where the sergeant was assigned. He said that the sergeant would be handsomely rewarded if he would supply information of interest. The sergeant said that this was risky, his career would be in jeopardy, but that he would think about it. He did think it over, and the next morning he reported the incident to his commanding officer.

The above episode actually took place and similar incidents will continue to occur.

Every officer, soldier, civilian employee, and dependent must know how to recognize and defend themselves against possible attempts at espionage or subversive activity. It is equally important to know what to do if an attempt is made to involve you in this type of activity. The first requirement is to be able to recognize situations that indicate a possible attempt involving subversive or espionage activities. Examples are as follows:

a. Attempts by individuals with known or suspected espionage, subversive, or FIS backgrounds or associations to cultivate friendship with Army military and civilian personnel or to place them under obligation to provide information.

b. Attempts by individuals to coerce Army military and civilian personnel to obtain military information for espionage purposes.

c. Attempts by the FIS to obtain classified defense information through observation, document collection, or personal contact with United States Army personnel and civilian employees.

d. Intimidation of DA personnel who are traveling to criteria countries.

e. Exploitation of personnel having a tendency toward disaffection or having personal difficulties.

f Threats of exposure of past or present indiscretions.

## USARAK Pamphlet 381-1

If you have any reason to believe that you or your dependents are the target of the FIS, report it to the Alaska Resident Office at 384-1622 or 172d Military Intelligence (at Fort Wainwright) at 353-9423. They will advise the appropriate intelligence or security office. DO NOT show that you are suspicious or change your manner toward the individual you suspect. Never agree to or sign ANYTHING! Remain noncommittal. Do not take action to exploit, apprehend, restrict, or stimulated further contact until a competent authority provides guidance.

We have just pointed out to you how to recognize attempts at subversive or espionage activity. Now, let's go on to methods of defending yourself against these possible threats. You can best do this by a few simple habits of thinking and acting, on and off duty.

- a. Be security conscious 24 hours a day.
- b. Know and strictly observe all security regulations affecting your duties.
- c. NEVER discuss classified information with unauthorized persons.
- d. Always remember that a person's clearance for a certain category of information does NOT entitle them to know everything in that category. It only authorizes them to have access to information they need to know to perform their duties.
- e. Avoid any kind of public or private conduct that might be used as a blackmail weapon against you.
- f. Be cautious in all new friendships, especially if they develop out of strange or unexplained circumstances.
- g. Avoid groundless or foolish suspicion. If you feel there are good grounds for suspicion, report them to the proper authority IMMEDIATELY!
- h. NEVER attempt any counterintelligence work on your own.

Past experience has shown that dependents have also been FIS targets. Therefore, you are required to brief your dependents on the methods used by the FIS and the necessity for prompt reporting should they become involved. It is only with the full cooperation of all personnel assigned, employed, or associated with the United States Army that we can successfully counter FIS activities directed against us.

## Chapter 5

### Sample Subversion and Espionage Directed Against the United States Army Briefing (Foreign Intelligence Service Exploitation of United States Army Personnel)

The significance of the findings resulting from research and analysis of data concerning the motivations of United States Army personnel who have defected to, or have engaged in espionage for, the FIS, lies in the simple, incontrovertible relationship between the individual's standards of personal conduct and a major United States Army security problem.

#### Personal Conduct and Security

A rather large percentage of the American public's books, short stories, television, and theater movies are successfully based upon a popularized theme of espionage, counterespionage, and subversion. James Bond (007), "True Lies" (Arnold Schwarzenegger), "Mission Impossible" (Tom Cruise), almost any Tom Clancy novel, and numerous other books, movies, and compact disk read-only memory (CD ROM) games have become common household terms. Just as some of these may fascinate the young (and not-so-young) admirers with science fiction-like equipment and unrealistic achievements, one might be led to believe that the espionage and counterespionage is an exciting, romantic, and honorable way of life. It is challenging, but seldom, if ever, romantic. It can be honorable, but NOT when a person elects to sell out their country, their family, and their friends, all for an impression that is far from the facts. In the latter case, the road is paved with fear and friendless frustration that leads to self-condemnation, hopelessness, and a bitter end to an alien environment.

Why do people become traitors? Why would anybody ever agree to spy for our country's enemies? Why would an American voluntarily leave his/her country for a life in a police state? Most of these persons eventually wake up and deeply regret their actions; often after it is much too late to save their ruined lives. But what circumstances led them into such a situation? Who are the individuals susceptible to these incriminating developments? What type of person would sell out his/her country and military associates?

The answers to these questions were sought through analysis of the cases of espionage, subversive activity, and defection by United States Army personnel, United States Army civilian employees, and their dependents since World War II. The facts and conclusions revealed are interesting and some are surprising.

One of the earliest areas checked was that group of personnel with foreign ties. Of particular interest were the cases of those persons—

- a. Who were born in, or had blood relatives in criteria countries.
- b. Whose wives were born in, or had blood relatives in criteria countries.
- c. Personnel who had strong ties in criteria countries, due to residence or other relationships.

This personnel category was of early interest. A known FIS technique involves coercion or pressure upon Americans selected for recruitment who have these foreign ties, by threatening to harm, or promising better treatment of, relatives living in these countries. In a sense, these relatives become hostages. The same pressure has been applied, along with promises of personal gain, to encourage Americans to defect to these countries. A defector, as used herein, is a member of the United States military who voluntarily leaves the United States control and physically place themselves under the control of authorities of a criteria country.

One might think that a foreign background or foreign relatives, coupled with the tremendous emotional pressures that the FIS can apply, would logically point to this group of United States personnel as the weakest link in our security chain. The facts belie such a hasty assumption. It is just NOT so! Perhaps their previous, direct exposure to the knowledge of the Communist way of life provides a better grounding for these persons to make personal and official decisions.

## USARAK Pamphlet 381-1

This analysis of all known cases of espionage and defection by United States Army personnel has confirmed that in no known case has an individual with foreign ties been successfully coerced to reveal classified information to the FIS by sole reason of those foreign ties. Likewise, in defection cases it has been established that foreign birth or relationships have not been a primary cause for defection. While some aliens in the United States Army may have been influenced to defect by an urge to return to a more familiar environment, this has been a secondary rather than a primary reason. Of the total defections by United States Army personnel since WW II, not including those Americans who refused repatriation after the Korean Conflict, 19.5 percent were foreign born. The majority of these were born in Europe, in Iron Curtain countries, and most of these had been alien enlistees under the Lodge Act, which was passed by the 81st Congress and went into effect in 1950. These individuals usually had relatively short exposure to life in the United States or United States military control, averaging less than 3 1/2 years.

What of the other 80.5 percent of the total number of defectors and the majority of those who agreed to spy against the United States for the FIS. These were American-educated personnel, who knew our way of life, but frequently knew very little about a life under a Communist regime. Were they converted to Communism as a prelude to their acts, and hence motivated by a burning dedication to the downfall of the United States Government? No. There have been spies against our government based upon such ideology, but not among the United States Army cases. United States Army personnel involved in espionage and defection cases were trapped! Trapped by their own conduct! Perhaps it seems ridiculous, but it is not; not at all. Case after case has revealed, almost with certain monotony, that misconduct is our greatest security weakness and that a clever, ruthless agent capable of detecting and exploiting these personal weaknesses capitalizes on this.

The common denominator so consistently present in both espionage and defection cases are directly attributable to a lack, or a temporary slippage, of individual self-control. This can easily lead to specific problems, such as sexual misconduct, gambling, or drug and alcohol problems. These factors, in turn, can lead to disciplinary problems and actions by commanders. This may spawn initial pressures on and resentment by the subject. Frequently, an immature attitude results in the individual's search for solace. It is found in a compounding of the original problems of conduct—the few extra drinks, the soft shoulder of a friendly listener, indebtedness from reductions in pay or overspending, ensuing marital problems, or the frantic attempt to "hit the jackpot" gambling. This person is ripe for a subtle, or even direct, approach by the FIS.

A large majority of the American-born defectors did have "foreign connections" in that they had foreign lovers or girlfriends/boyfriends who often accompanied the defector behind the Iron Curtain. But again, in these cases, the foreign connection was not the basic reason for the defection. The basic reason in virtually every case has been that the individual was attempting to escape the consequences of personal misconduct.

Approaches by the FIS have been made to service personnel visiting in Communist countries and through foreign spouses. Analysis has shown that the personnel with foreign connections have, in most cases, scrupulously reported these incidents to proper authorities, effectively negating FIS attempts under this technique. Hence, in the past, a foreign connection has increased the chances of an FIS approach; although it did not increase the chance of FIS success.

Analysis of espionage and defection cases in the Army indicates that other factors, such as indebtedness, moral misconduct, liquor, marital problems, and impending disciplinary actions were more proximate causes for defection and espionage cases than foreign relatives, association, or contacts.

Our existing personnel security regulations, properly implemented, will effectively weed out those not clearable for, nor eligible to retain, access to classified information. Certainly any foreign connections will be examined for security implications at the time of a background investigation. Favorable results are not an assurance that unfavorable situations or factors will not subsequently develop.

The greatest security threat to the United States Army is the person with a good record and background who turns sour. It has been found that cases of defection and espionage are almost solely attributable to

## United States Army Alaska Pamphlet 381-1

behaviors that are obvious or readily detectable and, therefore, susceptible to preventive measures by the command.

Two examples of "exemplary" soldiers who turned traitorous are the Clyde Lee Conrad and James Hall cases. Both were considered by their respective chains-of-command to be great leaders of soldiers. What lead them into a life of espionage? MONEY!!!—plain and simple.

Defections and espionage do not normally occur because of political conviction or conversion to Communism. One does not have to peer into a person's head or determine his/her politics to identify a potential defector or spy. The indicators are on the surface. If a person regularly misbehaves, either on or off duty; if they mismanages their personal affairs; or if their conduct is immoral, the potential for espionage or defection is greatly increased.

Analysis has shown that the defector is escaping the consequences of his/her behavior or mismanagement of his/her personal affairs. If he/she is in serious debt; if he/she is married and has committed adultery; if he/she is facing a court-martial or other punishment for misconduct, defection to a Communist country appears to provide a safe haven where he/she cannot be apprehended. Of the United States Army personnel who have defected, some have died under Communist control. More significantly, over half have returned; even they could not stomach existence under Communist conditions. In other words, although they were facing trial for desertion and almost certain conviction, imprisonment, and disgrace, they chose to come back and face realities. How much simpler it would have been to face them earlier, before they compounded their errors into traitorous action.

Analysis of espionage cases reveals that the FIS has found that the person whom they can most easily recruit is the one who has a personal weakness they can exploit. It is known that at least 20 percent of assignments given to FIS agents deal with the spotting potential recruits and assessing their weakness.

Even where a foreign connection may serve as an avenue of approach, the basic inducement stems from the exploitation of the individual's weakness. If the person is in serious debt, they are offered money. If he/she is preoccupied with the opposite sex, he/she is furnished with a match. If he/she is homosexual, he/she is sent another. If he/she is concealing misconduct, he/she is threatened with disclosure. Foreign connection or no foreign connection, these are the ways that spies are recruited. Foreign relatives or appeal to foreign birth or ideology seldom, if ever, are the key factors in a recruitment.

The FIS detects these weaknesses from the outside and exploits them. With proper reporting and detection, it is simpler for the United States servicemembers and their supervisors than the FIS to detect these individual weaknesses or problems of their personnel and prevent their exploitation. Supervisors at all echelons, military or civilian, must be alert to this threat and actively involved in its reduction.

A pertinent fact that should be noted is that the large majority of servicemembers involved in espionage cases are American-born who had favorable background investigations allowing them to be given clearances for access to classified defense information. Two recent cases were Harold Nicholson, a Central Intelligence Agency officer and James Hall III, an Army warrant officer.

Nicholson, a divorced father of three who wanted to compensate his family "for failing to keep my marriage together" worked as a station chief in Romania. He admitted meeting with his Russian handlers four times over a 2 1/2-year period. As a result of those meetings, Nicholson sold secrets as well as identities of other Central Intelligence Agency officers. He had received approximately \$300,000.00.

Hall was caught after he bragged to an undercover Federal Bureau of Investigation agent that he had sold top secret intelligence data to East Germany and the then Soviet Union. He said that he had been motivated by money. It was not that he needed the extra money, he just did not want "to worry where his next dollar was coming from." Hall is believed to have received over \$100,000.00 from agents of two different countries. One reason for his detection was that he was considered to be living far above what his pay scale would allow.

## **USARAK Pamphlet 381-1**

In all cases, spies and defectors alike, the following factors have been found to predominate, either singly or in combination:

- a. Excessive indebtedness or recurring financial difficulties.
- b. Homosexual, criminal, or immoral conduct.
- c. Excessive drinking or use of narcotics.
- d. Sudden, unexplained affluence.
- e. Questionable or unauthorized contact with representatives of foreign governments or agencies.
- f. Repetitive absence without leave.
- g. Mental or emotional instability.

In practically all cases, after-the-fact-investigations revealed that these indicators were known to someone before the individual's defection or detection of his/her involvement in espionage. In many cases, they were a matter of official record. Commanders already have the authority to take prompt action in instances where these indicators are present, under the authority of DA directives. The Chief of Staff has directed that when the indicators listed above are apparent, commanders must take action to suspend the individual's access to classified information. If in an overseas area, return the individual to the continental United States, even without prior DA approval if the situation warrants.

Consistent observation by competent leadership at all levels will provide the continuing evaluation to overcome character weakness, which is the greatest threat to our security. Further, discussion of personal and official problems by individuals with supervisors and commanders can avoid their magnification of the individual concerned, and forestall the ill-conceived, personal decisions that can only lead to tragedy.

## Chapter 6

### Sample Subversion and Espionage Directed Against the United States Army Briefing (Proof Positive)

NEWS BULLETIN! "Harold Nicholson, CIA intelligence officer, assigned to the CIA's counterintelligence branch in Europe, was arrested by agents of the FBI on November 16, 1996 the charge—espionage."

NEWS BULLETIN! "Nicholson was convicted and sentenced to 23 years imprisonment for his espionage activities."

Our purpose is to alert you to the ever-present threat of espionage and subversion directed against Department of the Army today.

Personal involvement by any one here today in espionage is considered a real possibility. It is possible that a person in this very room is presently working for the FIS.

It is because of this possibility that we review, at least once a year, the methods used by the FIS to gather information concerning the United States Army, its installations, activities, equipment, plans, and personnel.

Before we begin our review, it would be wise to define the meaning of espionage. Webster tells us that espionage is a word of German origin, and involves the use of spies, especially for military purposes. Espionage, if successful could cause the defeat of our country, the loss of our liberties, the death of millions of our citizens, or affect our way of life for decades to come.

On 16 July 1945, the first atomic bomb was detonated at Alamogordo, New Mexico. The atomic age began with the explosion of a bomb so powerful and destructive that some people speculated it would end war forever. On 19 September 1945, Klaus Fuchs—with the assistance of United States citizens, Julius and Ethel Rosenberg—obtained through the techniques of espionage, and transmitted to the Soviet Union, the complete plans and specifications of the atomic bomb. This act of espionage, as we all know, has changed the course of history and will undoubtedly affect the lives of Americans for years to come.

Nations have always cloaked their strengths and weaknesses in a mantle of secrecy as a defense against their enemies, both actual and potential. As a result, intelligence operations in various forms are initiated to obtain these secrets. Today every nation, no matter how small, has its own intelligence service. The energies of these intelligence services are directed against every nation, both friend and foe. Because of the extent of the intelligence gathering activities and to protect our defense secrets, security guard forces, high barriers, alarm systems, complicated safes, locks, and personal security investigations are all employed to this end.

However, the principal weakness in any security program, no matter how well conceived or aggressively pursued, is the individual. Because of this, the energies of professional, dedicated, well-trained FIS agents from all nations are targeting you. You are the principal target because you work for the military of our nation. Through you, they are capable of penetration of our security at the highest level and through you, gain knowledge of our most important and closely guarded secrets.

The FIS espionage network, augmented by the governments of many countries, encompasses the globe. Thousands of FIS agents, in the guise of diplomatic personnel, military attachés, commercial representatives, technicians, tourists, and émigrés carry on clandestine intelligence operations from around the world. Some are located in allied and satellite embassies, consulates, or the residences associated with these diplomatic installations. Others operate under the cloak of press or travel agencies and trade delegations. Still others illegally infiltrate other countries and pose as loyal citizens while covertly engaged in espionage activities.

## USARAK Pamphlet 381-1

In the Washington, D.C. area, for example, there several groups with the covert mission of attempting to obtain information concerning this country's military strength, disposition, training, equipment, communication systems, plans, weapons, and anything that would aid FIS agents if there are hostilities.

We must, without reservation, accept that FIS activities are extensive, their bases are all around, their professionalism proven, their capabilities in any area extensive, and their principal target is you.

In attempting to further their goals through you, they must first make an approach and solicit your cooperation.

The approach and recruitment of an individual by the FIS is not a haphazard endeavor, but an extensive, well-planned, carefully researched project.

The approach may be accomplished under a number of guises:

- a. The FIS agent might seek your friendship through a mutual interest, such as a hobby, an interest in the arts, a common professional background, or a myriad of other common interests.
- b. They may seek you out in a social situation, such as a club meeting or cocktail party, and later follow up the contact with an attempt to form an association of a more lasting nature.
- c. He/she may introduce himself/herself through a mutual acquaintance and seek your association in a more direct manner.
- d. They may attempt to contact you through the Internet.

Whatever the method, the goal will be the same—to meet you and, through this contact, learn all he/she can about you, your interests, philosophy, ambitions, weaknesses, and motivations. His/her need to learn about you is necessary to his/her next move: recruiting your cooperation.

To be of value to the FIS, you must be motivated to do their bidding.

Persons who become involved in espionage fall generally into four categories:

- a. The mercenary who operates solely for monetary gain.
- b. The person whose misconduct has led them to entrapment or fear of disclosure.
- c. The ideologically motivated individual who believes that the FIS's cause is more just than that of his/her own nation.
- d. The person placed under pressure due to compromise or threats directed against relatives in another country.

In assessing persons for use in their espionage efforts, the Communists consider the individual's personal habits, traits of character, and mannerisms. His/her associates are scrutinized to determine any irregularities of conduct. Information is sought regarding personal interests and associations with relatives and friends in other countries. Particular attention is given to individuals who drink to excess or become involved in illegal transactions, sexual misconduct, excessive indebtedness, or the improper use of narcotics. In determining how best to effect the recruitment of a potential source, the FIS considers no piece of information insignificant or irrelevant. Any evidence of misconduct is exploited to the utmost. If there is no evidence, it may be contrived. In contriving a compromise, an FIS agent will go to great lengths. For example, he/she may arrange a situation where the unwitting married United States military or civilian employee is lured into an illicit relation with a member of the opposite sex, and photographs are taken. The threats of exposure are sometimes sufficient to make a successful recruitment; while in other

## United States Army Alaska Pamphlet 381-1

cases, claims of pregnancy or alleged abortions are used to further entangle the victim. The contrived compromise used by the FIS is as varied as human weakness and is not confined to the male alone.

Today, the forces of the United States Army are deployed in every corner of the globe, as this worldwide development has been continuous since the early days of WW II.

A considerable number of United States military and civilian personnel married foreign nationals while stationed abroad, and through these marriages, have acquired close relatives living in criteria countries. There is a natural desire to visit or correspond with these people. There is no ban by the United States Government to prohibit persons from visiting or corresponding with these relatives or friends. However, the letters are subject to censorship by their authorities, and therefore pose a security threat to the individual. Persons who correspond with relatives or friends in criteria countries should not include information that could be used to assist these countries in their intelligence efforts. It should be remembered that the FIS will use everything and every possible means of approaching our personnel to obtain information about our strengths and weaknesses and, if possible, our secrets.

The following is an older case, however, it is still noteworthy because of the circumstances. Captain Walters, United States Army, married a Polish foreign national during a tour in West Germany. Mrs. Walters was an excellent FIS target for three reasons:

- a. Her mother lived in a Warsaw Pact country.
- b. She wanted to bring her mother to the United States, which required an exit visa.
- c. She was employed in the Visa Section of the American Embassy in West Germany and knew a number of émigrés from her own country.

After Mrs. Walters had applied for an exit visa for her mother, a Mr. Jobsky contact her, stating that he was from the Polish Legation. Jobsky seemed to be a friendly and helpful person. He stated that pending the possible granting of an exit visa for her mother, Mrs. Walters might like to visit her; in which case, he would help her in obtaining a visitor's visa, or she might like to send her mother parcels of food and clothing. All he wanted in return was a flow of information concerning Polish émigrés in the United States. Mrs. Walters declined to assist him. At this point, Jobsky, no longer friendly, stated that her obstinacy might have unfavorable consequences for her mother. Mrs. Walters had always expected such a day to arrive and had long since decided her attitude in the face of such blackmail. She remained firm. She informed her husband of the incident with Jobsky and they reported the incident to United States counterintelligence authorities. Mrs. Walters' courageous defiance cost her nothing. Her mother obtained her exit visa and was able to join her daughter and son-in-law in the United States.

Mr. Jobsky, and those like him, work for one goal and one goal only: to advance the aims of their causes and beliefs to our detriment.

As much as we may dislike it, we are living in a world during a time in which we must face a number of very disquieting realities:

- a. The FIS has one goal: their own countries' domination.
- b. They assume that their countries' domination will be accomplished by violent revolution.
- c. The Soviet Union was once regarded as the main force of this revolution, however, the revolution is more economically than militarily based now.
- d. In advancing these goals, the FIS uses the most modern and effective means of electronic warfare to strengthen their forces and lay the groundwork for economic and/or social revolution. One of the most effective and most often used weapons in their arsenal is subversion.

## USARAK Pamphlet 381-1

Subversion as practiced by the FIS is intended to weaken the faith of people in their government, and so undermine the government; thus preparing the way for revolution or possible take-over. The tactics employed in subverting a nation are varied; however, two principle techniques are always used:

a. The establishment of front organizations.

b. The infiltration by the FIS into established organizations and institutions at all levels of the target society. This illustrates the extent of their efforts in the United States.

There are as many worthwhile objectives and goals espoused as there are legitimate organizations. Many of these same objectives and goals are advanced by front organizations. The basic difference between front organizations and legitimate organizations is that the legitimate organization seeks to advance its objectives honestly for what its members think to be the good of our society and the front organization seeks to advance the objective or goal for one reason and one reason only: to lay the foundation for a take over by a foreign power. Many an honest and patriotic citizen has been startled to find himself/herself scheduled to appear or to be present at a front organization's rally when he/she thought he/she was participating in some worthwhile social or community activity.

All FIS home countries have rapidly expanding technology. As witness to this is China's recent joining of the nuclear powers and the Russian feats in space. The FIS has capitalized on this technology expansion and is using the fruits of this technology against us.

The miniaturization of electronic components in recent years has permitted the construction of self-contained transmitters. They can operate for weeks on simple power cells and transmit conversations in a room to a remote receiver several miles away. The FIS agent has only to enter the target area once, hide the transmitter in a sofa, chair, desk, or any inconspicuous place and return to the listening post. Transmitters can also be concealed in gifts such as bookends, clocks, ashtrays, pen sets, and many other items. One of these could be sent, for example, by mail to a person in the target area and the recipient would be unaware of the gift's real purpose. Other transmitters have been developed that use the existing 110-volt power sources as a receiver at another location in the building and monitor the target area for an indefinite time. The transmitter emits a signal that can be detected with proper receiving equipment; because of this, a countermeasures team can locate and neutralize a clandestine transmitter operating in a secure area. Periodic inspections by a countermeasures team will help in maintaining the security of an area.

Technology has also given us surveillance camera equipment so smart that it is hard to detect with the naked eye. These cameras are smart enough to be hidden inside small appliances and corners of rooms, as well as small open spaces, such as heater ducts. The actual recording device does not have to be attached to the lens, as we can see in medical operations. The lens can be of varying lengths, with the recording device or monitor several inches to several feet away.

The last electronic surveillance device we will describe is the miniature microphone.

There are many in use today. Their small size enables them to be concealed in virtually any area; and, when installed by a trained agent, they are practically impossible to detect by ordinary means. A small microphone installed in a desk, conference table, or wall can easily pick up and carry to a distant listening post all conversations taking place in the room. A microphone, together with a miniature tape recorder or transmitter, can be concealed in a briefcase or purse and left in the target area; or, as in many cases, carried by the agent into the area. The microphone does not have to have external wiring linking the microphone with the monitoring equipment. For this reason, they are often difficult to detect. If the FIS has this type of sophisticated equipment, then playing music, running water, or static in the background is not going to keep the FIS from hearing the conversation. They can have the noise filtered out through computerized filtering devices. Good physical security is the most effective method of safeguarding an area against the installation of clandestine listening devices. This, along with periodic technical inspections by countermeasures teams, will provide maximum security to sensitive work areas.

## United States Army Alaska Pamphlet 381-1

Besides the use of listening devices, photography is also used as a tool of espionage.

Miniaturized cameras have been consistently used by the FIS to photograph classified documents and sensitive installations, as well as personnel and equipment. Their small size affords an FIS agent many possibilities for concealment.

Take, for example, what appears to be an ordinary pack of cigarettes. Concealed within is a small camera, capable of taking many photographs without manually advancing the film. After the picture is taken, the film is automatically advanced to the next frame and the shutter is cocked by a spring mechanism in the camera.

A camera equipped with a telephoto lens can take photographs of a person or a document located a great distance from the camera. As you can understand, anyone in an open or even semi-enclosed area is vulnerable to such photographic techniques. A telephoto lens attached to a movie camera can photograph lip movements or persons discussing classified information without their knowledge. This technique has proven to be extremely useful when the agent could not place a listening device in a target area. Care should be taken when using classified information in an office to close off all avenues of visual access, to negate the agent's use of telephoto equipment. All the technical devices discussed here are commercially available and unfortunately, the agent can obtain them without risk.

We have just explored together some of the techniques that an FIS agent uses in furtherance of their ultimate goal. This goal, as tersely put by Khrushchev, is to bury us.

AR 381-12 requires each of us to report promptly to our nearest counterintelligence office any known or suspected activity of the FIS directed against United States Army personnel or installations.

Things you must report are:

a. Attempts by individuals to obtain classified United States defense information through observation; document collection; or personal contact with United States military, civilian, and dependent personnel.

b. Attempts by individuals with known or suspected espionage, subversive, or FIS backgrounds; or associations to cultivate friendships with United States military, civilian, and dependent personnel; or to place them under obligation for the purpose of obtaining information.

c. Attempts by individuals to coerce United States military and civilian personnel to obtain information for espionage purposes.

d. The intimidation of United States Government personnel either traveling to Russia or any other criteria countries.

e. The exploitation of United States military and civilian personnel having tendencies toward dissatisfaction or having personal difficulties.

f Threats of exposure of past or present misconduct.

g. Appeals made to United States military and civilian personnel to provide information to other countries of the free world.

Do not think because your work is unclassified that you are of no interest to the FIS. Every Army employee has knowledge that a foreign government would like to know.

Each of us has a responsibility to defend our country against the ever-present activity of the FIS. This responsibility can best be met by adhering to the following rules, both on and off duty:

a. Be security conscious every day—24 hours a day.

## **USARAK Pamphlet 381-1**

b. Know and observe all regulations affecting your duties regarding proper classified material handling.

c. Never discuss classified information with unauthorized persons.

d. Always remember that a person's clearance for a certain category of classified defense information does not entitle him/her to knowledge of everything in that category. It only authorizes him/her to have access to information he/she needs to know to perform his/her duties.

e. Avoid public or private conduct that could be used to blackmail you.

f. Never attempt an investigation on your own. This is a complex and highly dangerous undertaking that only trained investigative personnel can handle successfully.

g. Avoid groundless or foolish suspicion; but, if you see or hear something suspicious, report it immediately to your nearest counterintelligence office. Tell no one else.

The circumstances under which you may gain knowledge of FIS or subversive activities might be personally embarrassing. Embarrassment is a temporary thing, but the results of your failure to perform a citizen's duty may have tragic ramifications affecting your life and those of countless other Americans.

## Chapter 7

### Sample "Terrorism" Briefing (Profile on Terrorism)

The United States Army's concern over terrorism has risen over the last decade because of the steady increase in the number of terrorist attacks against United States citizens and interests. This rising concern has prompted the Army to establish an anti-terrorism information program for ensuring that all personnel are informed about the terrorist threat and measures that you can take to recognize and reduce this threat.

Anyone who is a victim of violence, whether it is done by common criminals, insane people, or local street gangs, may feel terrified and, as a result, may consider themselves to be the victim of terrorism. We, however, use the word "terrorism" in a much narrower sense.

Acts of terrorism are aimed at a larger audience than the immediate victims. The terrorist wants to have a psychological effect on some element of society he/she is attacking, to bring about the desired change.

This means that in most cases, a primary consideration for terrorists is how to ensure that their message gets to a larger audience. To do this, they often plan their operations to attract news media attention. They rely on the media to broadcast information about their acts to the audience they want to affect.

News coverage, regardless of its intentions, tends to magnify the threat from terrorism and publicize the cause of the terrorist. This aspect, the intent to influence a larger audience, is what differentiates terrorism from other acts of political violence, such as the assassination of a political figure by his/her rival.

The threat to United States interests worldwide is higher today than it has been at any time in history. Evidence suggests that terrorism will continue to pose a threat to the United States military for the foreseeable future. It is important that all Department of Defense personnel be aware of the terrorist threat that exists in the countries where they are assigned or planning to travel.

Having examined the worldwide terrorist threat, we would like to discuss terrorism from the perspective of personal security.

Too often people do not take basic precautions to counter the terrorist threat. Army personnel who do not actively follow a security program place their lives in unnecessary danger. The number of terrorist attacks against United States military installations and personnel has increased significantly. In fact, the number of attacks against the military is increasing at a faster rate than the attacks against other targets. Keep in mind that from 1968 to 1984 there were 810 international attacks against the United States military.

The Department of the Army is concerned over the growing threat of terrorist attacks on its personnel wherever deployed. The Army recognizes that we are soft targets, normally undefended as well as publicly accessible; and, in many overseas areas, a highly visible manifestation of the United States presence. Consequently, we are susceptible to the terrorist as victims of circumstances—being in the wrong place at the wrong time; as targets of opportunity; or as selected targets of significance. To combat such a threat, you must maintain a constant state of vigilance. If you study the patterns of terrorism, you will become much more capable of thwarting terrorists than the individual who remains complacent.

The objective of this portion of the briefing has been to impress you with the fact that the terrorist threat is real and it's up to each and every one of us to be security conscious and report all suspicious activity.

Any person (soldier, dependent, or Department of the Army civilian) leaving the United States on temporary duty, permanent change of station, leave, or any other reason, is required by AR 525-13 and Department of Defense Instruction 2000.16 to have antiterrorism/force protection training within 6 months of leaving. Level I training is good for 12 months following the briefing, and Level II is good for 6 months. This training is provided from the Alaska Resident Office, 384-1622.

**USARAK Pamphlet 381-1**

FOR THE COMMANDER

OFFICIAL:

CHARLES R. DEWITT  
COL, GS  
Chief of Staff

//Original Signed//

WILLIAM F. HIGGINS, JR.

LTC, SC

Director of Information Management

Distribution:

B Plus:

25 - APVR-RIM-ASD-PB

5 - MOS Library (Building 600, Fort Richardson)

5 - MOS Library (Army Education Center, Building 21-10, Fort Wainwright)

3 - APVR-RIM-ASD-WB

2 - IAGPD-MID-ARO

1 - APVR-GPA-AE (MOS Library, Assistant Directorate of Community Activities, Education Branch,  
Attention: Mr. Mauer)

1 - Commander, United States Army Pacific Command, Attention: APIM-OIR  
Fort Shafter, Hawaii 96858-5100

**Appendix A**  
**Recommended Reading**

For additional information on the threat of subversive activity and espionage against the United States, the following list of publications is furnished as recommended reading:

Title	Author	Date
1. Nightmover	David Wise	1995
2. Family of Spies	Peter Earley	1988
3. I Pledge Allegiance...	Howard Blum	1988
4. America's Secret Army (Counterintelligence)	Ian Sayer and Douglas Botting	1989
5. The Second Oldest Profession	Phillip Knightley	1988
6. Catching Spies	HHA Cooper and Lawrence J. Redlinger	1988
7. Territory of Lies	Wolf Blitzer	1989
8. Spy vs. Spy	Ronald Kessler	1988



**Appendix B**  
**Subversion and Espionage Directed Against the United States Army Films**

Title	Length
The Falcon and the Snowman (1984, Orion)	131 minutes
America at Risk: SAEDA	22 minutes
Espionage Alert (A1104-91-1094-01-A01)	18 minutes
The Dark Side of Espionage (505183)	20 minutes
Hard Target (803455)	16-1/2 minutes
Antiterrorism/Force Protection Training (710951)	83-1/2 minutes



**Glossary**

AR.....	Army Regulation
CD ROM.....	compact disk read-only memory
CIA.....	Central Intelligence Agency
DA.....	Department of the Army
D.C.....	District of Columbia
FBI.....	Federal Bureau of Investigation
FIS.....	Foreign Intelligence Service
KGB.....	Komitet Gosudarstvennoi Bezopasnosti
SAEDA.....	Subversion and Espionage Directed Against the U.S. Army
U.S.....	United States
USARAK.....	United States Army Alaska