BASIC SPY TRADECRAFT

Internet Excerpts from the world of Spycraft

Edward Howard Lee

BASIC SPY TRADECRAFT FOR THE TRAVELER , BY EDWARD LEE HOWARD

While the principles appear quite basic and common sense-like, spycraft--and counter-espionage--is an art like winemaking and is practiced by professionals with many years of experience.

So you are on the road to a new city, and you plan to have a discreet rendezvous with someone, get in and out without being noticed, or just lay low. What must one do? How must one act? Most important, how must one think if they are to accomplish their objectives?

Plan where you're going. Know the area even if it means simply studying a map. Scope out the venue for a meeting ahead of time. Identify the exits, know the operating hours. Always think about how the opposition would approach you if they find you there.

The old boy scout motto "be prepared" best summarizes what is needed here. Mental state is the most overlooked principle in spycraft. It is not enough to say one must be cool under fire. You must always be prepared for the worst and be 100 percent prepared with a contingency plan. What if the person you're meeting doesn't show? How will you discreetly arrange another meeting? Why didn't you have an alternative meeting place at the time?

A spy doesn't do anything without a carefully worked out plan to include contingency and escape. Operating while being watched is bad business for a spy. Would you still meet your voluptuous secretary at an inn outside Prague if your spouse showed up outside as you approached? Probably not. But if you are a spy, you would already have a contingency for evasive action.

There was a World War II maxim, "There's no such thing as too much security." Assume walls have ears, assume you're being watched until proven otherwise, and assume your briefcase will be examined when you leave your hotel room. If you always expect the worst, you'll be better prepared for it. Don't be sloppy with security. If your enemy suspects you're up to something he will take counter-measures and try to catch you off guard.

Don't trust anyone! Don't trust your wife or your girlfriend with the information you've been sent to Vienna to have a secret meeting. They may love you dearly but their loose telephone chat could blow your mission. Remember the axioms "need to know" and "what they don't know can't hurt you."

PART ONE: DETECTING SURVEILLANCE

Knowing whether you are being followed or watched is a basic element in any espionage activity. There's no point being a spy if your opposition follows your moves and know what you're up to. You would then become an instrument of the opposition, subject to manipulation. In the history of espionage, numerous spies have been identified by counterintelligence services and not arrested but duped.

On foot: This is the hardest and can only be mastered after several weeks of practice in streets, stores, parks, alleys, entrances and exits from buildings. Professionals practice for hours against counterintelligence teams.

- Be observant without staring or rubbernecking.
- Pay attention to faces and clothes, particularly shirts, coats and shoes.
- Design a Surveillance Detection Route (SDR) that is both logical and will force the opposition to show themselves.
- Remember: "Once is coincidence, twice is enemy action."

Design your SDR to take you to at least three different places in different areas of town. The last stop should be somewhat provocative—perhaps an alley leading to a small store, compelling your surveillance to wonder what is going on and follow you, allowing you to identify a face your observed earlier.

Know in advance what you will do if you confirm surveillance: Go home—or jump into a taxi at the store's rear entrance.

A warning: Almost nothing will work against a large team of professionals if they want to stick with you. I had almost 60 FBI Special Surveillance Group on me in Santa Fe in 1985. The KGB in Moscow sometimes mobilizes 200 persons on one suspected CIA officer. Against such

manpower, it it time to go home, while remembering the words of Yakov Peters, Deputy Head of the KGB in 1918: "The best quality of a spy is patience."

By automobile: Conducting an SDR in a car is easier than on foot. Cars cannot change clothes and are easier to spot without turning around i.e. through your rear-view mirror. The principles are the same: Visit three spots with an obvious reason (bank, cash a check; laundry, drop off clothes; grocery store, pick up snacks). Keep track of the types and colors of cars at all three places—tag numbers, if possible. Decide, are you clean or not. If clean, move onto your rendezvous.

Public transport: Old spy movies love to show the scene where a man gets onto a bus and steps off at the last moment before the door closes to see if someone else tries to jump off. This is a bit exaggerated, but demonstrates an important principle of good SDR: You always want to channel your opposition into choke points. Cross a small bridge in a car, up an alley by foot, into a bus where you can isolate and identity.

The operational site, if you have decided you are clean, is obviously the most important part of your trip. You've come all the way to Vienna to meet someone in secret. The effort you made paying your ticket in cash, inventing stories for your spouse and boss, and your SDR stops along the way, have finally brought you to your destination. It is therefore important that you've chosen a good venue for the dirty deed.

PART TWO: COMMUNICATIONS

Signals and other types of covert communication are necessary for secure contact with your conspirators. Signals, while traveling, can be visible and verbal. Normal covert communications are the coded letters or secure telephone chats you may have with your conspirators. These normal communications are not done while you are traveling.

Signals are covert communications that you might use with your conspirators when you both approach operational activity. In other words, you've arrived in Budapest and are set to meet someone within 24 hours in the park near Margit Hid Thermal Island Hotel. The meeting was set up a month before and now you're ready to signal your agent, "I'm here, ready to meet according to plan." You also want to hear from him likewise that he's okay and will attend the meeting. Thus you both have a signal plan.

Stationary signals: The classic. Perhaps a chalk-mark on a billboard. A pot of flowers by the window. An orange peel tossed on the path near your hotel (an old KGB favorite in the USA!) Use your imagination, but don't get too exotic or draw attention upon the signal itself.

Moving signals: Perhaps you drive by a specific bus stop known to your agent at a specific time. Or perhaps you stand at a specific street corner for five minutes where your agent can see you from a high-rise building nearby.

Verbal: The most dangerous sign because it usually means you and your conspirator need to be in contact. That's bad if anyone is paying attention. Example: Calling your conspirator's office with a phony message i.e. "Please tell Mr. Smith it's time for his annual dental exam." Never use a phone from your office, residence or hotel! Always use street phones [these days, pay-as-you-go cell phones]. But remember, these are also subject to tapping by the professionals. For this reason, professionals use the telephone only in extreme situations, such as a danger signal. This tells your conspirator to get out or go on ice. The risk of a phone call is merited only by such a situation.

Good spies always think first about the hot water their agents can get into by poor planning. It can result in a blown agent. Always analyze your plans from the perspective of your agent's security. Make life easy for your agent. If he's a professional person, don't ask him to meet in a dark and dirty bar in the wrong side of town. Maybe *you* fit in, but *he* doesn't. Identify meeting places where your contact has a good reason to be present.

A good "Commo Plan" (communications) is necessary for any long-term relationship. The plan should be developed after reviewing your own lifestyle and that of your agent. You'll probably be flying in to see your agent every quarter-year. Make plans in advance for meetings: places and times. Arrange signals. Have danger and escape contingencies.

You, the intelligence officer, must take the lead in drafting the plan, then reviewing it with your agent to make sure he or she a) understands it completely and b) is comfortable with it. Write the plan down, analyze it together, and commit it to memory. Any brief notes should be well hidden and make no sense to anyone who might read them.

In espionage, Murphy's Law applies double!

If something can go wrong it will go wrong. I have worked with CIA, FBI, and KGB officers who told me countless accounts of how their "perfect" plan for meeting went wrong at the last minute. The resourcefulness and a creativity of a spy to think fast on his feet and invent new tactics are primary for success.

PART THREE: TRAVEL

Airline reservations: Airline computers are bad for the spy. They leave footprints of where you went and when. If you have fake ID documents, it is best to use your travel alias and make reservations from a public phone [ed: or these days, from a pay-as-you-go cell] not near your home or office. If you do not possess fake documents, travel part of the way under alias. If, for instance, if have to travel from Miami to Vienna, make a reservation from Miami to New York under an alias and make a true name reservation from New York to Vienna, as passports are checked. (Ed: These days, of course, one cannot board an internal US flight without ID—take a train or bus.)

It is best to pay cash for your tickets; credit cards also leave footprints.

Wherever possible, use smaller foreign airlines, which are generally less available to those checking computer reservations. For this reason, KGB officers always preferred Malev (National Hungarian Airlines) whenever they crossed to Europe.

Once inside Europe, it is best to take the train anywhere and everywhere. Border guards on trains often do not have regular access to computers for checking passports—though watch out, some now carry laptops!

So, let's say you're traveling to Europe for a secret rendezvous:

- Do not fly directly to the city of your rendezvous. Fly to another and spend two-to-three days checking for "shadows" before proceeding to your target area. Approach your target area with caution, by train. Make hotel reservations at the last possible moment from your first European stop. Even better, find a place to stay once you arrive.
- Allow yourself a day or two in the target city to familiarize yourself with the town and rendezvous site. Keep a low profile; develop an escape plan.

PART FOUR: TOOLS OF THE TRADE

This is about the gadgets and devices a good spy may want to have in hand for a dangerous rendezvous with his mistress in Vienna or an inside connection at a Swiss bank in Geneva. My fascination with gadgets began with James Bond movies in the 1960s. Bond had many goodies, from an exploding briefcase to an Aston Martin with an ejection seat for the unpleasant passenger.

There are some standard if less extravagant items you may want to consider for your mission. Ideally, these are items that are helpful to you in the execution of your mission but will not attract attention if found in your luggage by a Customs inspector.

Good spies like to go unnoticed, know what the opposition is doing, be able to switch identities, have good *commo* with agents, and be prepared for all eventualities, including emergencies. What tools or gadgets will help with that?

Let's start with disguises: They run the gamut from wigs and mustaches to full-blown face masks. But also includes glasses and different clothes (try as cleric's collar). In short, whatever it takes for the opposition, which already knows what you look like, not to recognize you. The number one rule with disguises: Do not choose one that attracts attention. Don't wear that clerical collar to a nude beach! Don't wear sunglasses in the rain! And don't wear a cheap mustache past an Immigration inspector! In fact, never wear a disguise past police or immigration unless it is a dire emergency. It if can't be done right, don't do it. Nothing looks worse and attracts more attention than an amateur wig or fake mustache. I'll never forget the time I met a CIA instructor on a training exercise in Virginia and my mustache started coming off as I ate soup in a restaurant. (I'll also never forget jogging through a park in Washington DC with a black man's face mask and being called by a group of black teenagers to join them in game of basketball—one of my positive disguise experiences.)

The simpler the disguise the better. You'd be surprised how a simple pair of glasses can change your appearance. Or how much just combing your hair a different way creates a new you. Combine both and you've altered your facial appearance quite a bit.

Now for the body: Carry a brief-bag with a jacket and pair of shoes inside. Change in the restroom; anyone watching would probably not recognize you coming out.

Next, documents: As a tool of the trade, documents are important and can get you out of jams. But like a bad disguise, nothing stinks more than a poor document. Cops and Immigration officers are expert at spotting them.

Ancillary documents--club memberships, Library cards—are good for faking laymen and are good back-up for fake ID such as drivers licenses. They'll get you past janitors and doormen—but not into an ICBM site.

Genuine phony documents for international use, such as a passport, take time and money. Best bet is an expensive second passport from a country like Paraguay or Costa Rica.

Third, gadgets: A technical gadget will never replace good human planning and ingenuity. Many a spy has been caught because he or she has relied too much on their gadget.

Some good gadgets:

- Scrambler telephones to encode your chats
- Radio scanners to listen in on your opponent's radio chats.
- Night vision glasses.
- Lock picks.
- Miniature cameras; infrared cameras.
- Miniature transmitters for eavesdropping.
- Recording devices.
- Fake car tags.
- Paper dissolvable in water.
- Devices for concealing documents.
- Miniature copying devices.

Analyze your mission and determine what is truly necessary for accomplishing your objective. Don't believe the more you spend on gadgets the better a spy you'll be. Buy and take only what you need--the simpler the gadgets the better.

Secret compartments in brief-bags can be created by anyone with a flair for leatherworks and sewing.

Signal tools: These are items you will need for commo between you and your agent to signal: "I'm in town and ready to meet" and "I have left a package for you at site X."

Two principals about signals:

1. KISS. For "keep it simple, stupid." The simpler and easier a commo plan, the easier to execute it.
2. Signals must appear natural. A tossed orange peel near a newspaper vending machine is always better than a red flag in your window!

So, your tools: Chalk, bottles caps, orange peels—and tacks for sticking on telephone poles. Have these tools with you before you travel; don't wait to buy them when you need them.

I have traveled a lot in Central Europe. There is a standard list of things I take when I travel.

First, normal items, regardless of the purpose of my travel:

- Umbrella;
- Pen & paper;
- Swiss Army Knife;
- Sewing kit;
- Basic medicine (aspirin, Pepto-bismo, etc.);
- Reading material;
- A photocopy of my passport, kept in a place separate to my passport;
- Travelers checks, in addition to cash and at least one major credit card
- Snacks;
- A city guide to where I'm going.

If I were to visit Central Europe on a spy mission, I take the above plus…

- More detailed information on the city and a good street map;
- Contact information for my agent either memorized or written in personal code;
- More cash;
- A good legend about the purpose of my travel (sometimes "tourist" doesn't cut it);
- Dress and casual clothes;

- Binoculars;
- A gym bag (great for carrying extra clothes for a quick change to evade surveillance);
- A Polaroid camera (great for taking shots of targets, drop sites, etc.)
- A second set of documents kept in a safe place;
- A feasible escape plan based upon not returning to my hotel to collect my things.

Emergencies:

They happen when least expected. Be prepared.

Back-up support from home: A key person, such as your spouse, should be ready to wire money via Western Union.

Assuming your mission does not violate U.S. federal law, you may want to register your presence at the nearest U.S. consulate upon arrival in a foreign country. But be careful, American diplomats are not always discreet.

If possible, stash extra cash and documents in a safe deposit box at a local bank in the event you cannot gain access to your belongings.

Always approach your hotel as if someone may be laying in wait for you. You want to see them first, and then make decision about going in or taking off.

If confronted, remember the CIA Camp Peary mantra: "Admit nothing, deny everything, make counter-allegations." You would be surprised how many people allow themselves to get put on the defensive by counter-accusations! I once crossed into the USA on a false passport and the U.S. immigration inspector stared at my passport and seemed to think something was odd about the different levels of print texture in my false name. I got scared. And I said, "If that's a phony passport, I want my thirty-five dollars back." He laughed—and let me pass.

Finally, in a crisis remember the old John Wayne adage: "When the going gets tough, the tough get going." That may sound trite, but you can be your own worst enemy in a crisis if you panic. You can also be your own savior if you think calmly and logically to figure a way out. Good luck!

SPY'S COOKBOOK, BY EDWARD LEE HOWARD

CHAPTER ONE: MAKING THE DECISION

Making your decision to steal or divulge secret information for whatever purpose—money, power, revenge, sex, self-esteem—is one of the most serious decisions you will ever make!

You had better think long and hard on this matter because while you may envision yourself in Rio sipping a cool one you could instead end of sharing a cell with Aldrich Ames. As Clint Eastwood put it in Dirty Harry, "Do you feel lucky, punk?"

The step you take by selling one little secret is irreversible! As someone once said, "There is no such thing as being halfway pregnant." Neither is there any such halfway point in espionage. You gave out secrets or you didn't. It's that simple when the jury meets. You cannot plead extenuating circumstances, policy disagreements, conscientious objections, the harmlessness of the secrets, or that your wife needed more money or she'd leave you. Furthermore, someplace in the world there will probably be a memo of payment to you. Many former East German are being caught still after years of analysis by Western powers of East German Secret Service records captured after the fall of the Berlin Wall.

Your decision should be made in a cold and calculating manner. Look at the actual costs (operational expenses), potential lifelong costs of being caught (jail, maybe getting beat up), and finally the benefits. One thing is paramount in this analysis: your lifestyle will probably change whether you succeed or not. If you run with the money to Rio, you may be rich but you will probably never be able to return home. If you end up in jail, you won't be home either.

When one looks at the men and women who were caught it is surprising that most had no long-term plan in mind. Most were caught within months. Those who lasted years like Ames and Walker also did not possess a long-term plan. They apparently thought they could go on selling secrets forever. Remember this: "You can fool some of the people some of the time but not all of the people all of the time." Hence, make a plan for a drastic change of lifestyle within a specified period of time. It's like playing the stock market. One doesn't buy Microsoft thinking it will always go up. You buy in at a good price and, based on analysis, you have a target price. Same with espionage. Think over how long you can reasonably get away with it before someone launches an investigation, and plan where you want to be when they come

knocking at your door. That could be days, weeks, months or years—but never a generation. Think of it as a short-term business project with some prospect of profit and good prospect of risk. Once you make the decision to go for it, your job is to focus on increasing the profit side while reducing the risk.

One thing I remember well from my CIA days is that Murphy's Law applies double in the espionage business. If something can go wrong, it will. Plan accordingly. A case in point is the Russian defector Mitrokhin, a former KGB librarian who in 1999 published his secrets in the West. In his book he identified a British lady who cooperated with the KGB during the 1950s. I watched this lady on BBC News—a grandma about 85 years-old—come out of her house to meet the press and admit the truth. The last thing she expected was to be outed as a KGB spy 40 years after the fact!

CHAPTER TWO: MAKING THE APPROACH

You cannot imagine how many would-be spies got caught before even starting business. The most hilarious case was of a CIA officer who worked in the Cartography Office (maps). He decided that his secret level maps would be worth money to the Soviets but could not find a good way to approach them. Finally, he walked by the Soviet embassy and tossed a package of sample maps with his offer of employment onto the embassy's front lawn. Murphy's Law then took hold. Soviet guards spotted the package, thought it might be a bomb, and called the police. The police picked up the package, and the FBI picked up the would-have-been spy.

This brings us to the first rule of making contact with your prospective client, be it a foreign power or your company's main competitor: Assume the place you might want to make contact is watched and bugged. You will therefore want to make the approach in the most impersonal way possible. Use of disguises, a legend for being present—and leave your car at home. Better not to make contact at the prospective client's embassy or offices. Find out which bars and delis its officers frequent, and try to contact them there. Never use the phone!

The second rule is to make an untraceable offer. In the case of the CIA map man, the FBI immediately knew they could limit their suspected in a handful of people in a particular office. I was there once and did not see more than 15 people at work—but maybe that changed after the U.S. mistakenly bombed the Chinese Embassy in Belgrade using one of their maps). The best offer is verbal, made one-on-one, in an unthreatening location—like a "chance" meeting at

a bar. If you want to leave a written document, ensure that it is "clean" i.e. no fingerprints, no handwriting, not your own printer, and gives no specific information that can be traced back to you or your office.

Have a plausible excuse for your approach. For example, if you wish to visit the Cuban Interests Section in Washington DC, go ostensibly to enquire about tourism investment or the lifting of restrictions of the sale of medical supplies. Have back-up documents. If questioned afterwards, you've got something credible to show.

Finally, take your time, be patient with your approach. Yakov Peters, deputy to the very first chairman of the KGB (checkists) once said, "Patience is the best quality of a spy."

Await your opportunity. Never rush it. If you commence your approach and things don't seem right, break it off and return another day. Better safe than sorry, for in this case sorry may last for many years.

CHAPTER THREE: DEALING WITH YOUR CLIENT

This is a business deal. You have information for sale and they are buying. You want the highest dollar for your wares and they want the best information for the lowest price and trouble. Naturally, before dealing the buyer will want either a sample of the data you are offering or at least to know for certain you have access to such data. Be prepared for this in the first meeting.

The special nature of your business proposal requires that you seek special considerations in your relationship. Namely, you will probably go to jail if caught, hence you need special protection in your dealings. First, and foremost, you want them to understand your need for security. Whether you are dealing with the marketing director of a corporation or the First Secretary of the Russian Embassy, you will want him/her to be very concerned about your need for safety. If possible, conduct your business with one person (the fewer witnesses the better) and impress upon that person your need for safety.

Do not allow them to call you at home or work unless it's to tell you to get out and leave the country! Watch for the attention they pay to security. If they want to meet you at the café near

their office, they're being sloppy and not looking after your needs. If they seem indifferent to you at meetings, you can bet they won't care if you land in trouble.

Your dealings with them require special forms of compensation. Obviously, direct deposits to your bank account are out of line. The best deal is cash and/or a deposit in a secret account outside of the country in which you live. If they want you to sign a receipt for cash, never do so in a real name. Ask to use a false name for signing receipts and even then use a style of writing unusual to your own.

Finally, get straight with your client what is expected of them if things go wrong. If a foreign power tries to extradite you will they grant you political asylum? If you are dealing with a commercial client and you get fired will they hire you? In the mid-1980s, a U.S. Naval Intelligence analyst named Jonathan Pollard got caught selling secrets to the Israelis. He fled to the Israeli Embassy in Washington, onto to be refused entry and thereby turned over to a waiting FBI team. Tell me he was not a little disappointed!

CHAPTER FOUR: SECURE COMMUNICATIONS

If you do not have secure communications with your client you do not have a secure relationship and could very well end up in jail. Whether dealing with a foreign power or a commercial enterprise, communications is one of the most important elements of the relationship. Espionage books written by David Wise, Peter Wright, and Pete Early are full of pages about how the FBI was cleverly watching and listening as their most famous targets communicated with their clients. In some cases, the FBI caught on only long after the relationship had started and arrested the spies.; in other cases, the FBI intercepted the spies at an early stage and almost controlled the communications. I'll never forget reading about the tape of Rosario Ames calling her husband an "asshole" over the phone because he would not puck up from a Russian dead-drop.

If you are dealing with a foreign intelligence service, they will want to instruct you in this area. The CIA actually takes some of its best agents to a third country for a few days training. (The term agent means you, not the case officer.) I spent several weeks in basic officer training and then attended a special six-day course in Denied Area Communications to enhance my skills in preparation for my Moscow assignment. It all comes down to practice, practice, practice.

Here are the basic principles for secure communications:

1. Stay away from the telephone and assume all are monitored.
2. Have a reasonable "cover legend" when meeting your client.
3. Take precautions to observe if you are followed to a meeting.
4. Try to control the access area to a meeting.
5. Have an escape plan if things go wrong.
6. Keep materials for the meeting as "clean" as possible in case they are lost or confiscated.
7. Don't believe that because you are out-of-country you are safe. Many infamous spies have been under surveillance by the FBI or a friendly country's intelligence service while abroad (e.g. Boyce).
8. Use of other communication methods: Encrypted e-mail, cryptographic phones. These are fine against private security companies but will lose their value the first time the FBI discovers they're being used. They'll call in their in-house computer experts or even the National Security Agency to crack a sophisticated code.

CHAPTER FIVE: HOW TO HIDE YOUR MONEY

This chapter assumes you are trading information for money, and will save you a headache or two. Financial instruments range from cash to paper representing bank accounts, stocks, bonds, property, etc. to actual possession of rare metals. Some are liquid and untraceable and some are not liquid and very traceable. Cash or semi-secure bank accounts are best. I say semi-secure because the CIA and NSA can penetrate banks through computers. Back in the early 1980s a major intelligence service even sponsored the setting-up of a Swiss bank to have its bogus bank become a "member of the club." The rationale being that other Swiss banks share client data freely among club members.

The cardinal rule is to assume that if an investigation has been launched against you, your credit cards and major purchases (homes, cars, boats) will be subject to scrutiny. This poses a dual threat. If they can't nail you for selling information then perhaps the IRS can nail you for income tax evasion. The Rick Ames case provides the best example of poorly hidden money. The huge expense of his home, Jaguar, credit card balances and lifestyle on a bureaucrat's salary was a dead giveaway. If you do not move to Rio or can present proof of a large inheritance you had better not alter your lifestyle. So if money is your main

motivation, understand up front you may not be able to spend it for some time to come without great risk. This is important as we usually accumulate money for what we can buy—a better home, a better car, nice vacations.

Okay, you say, I cannot live high on the hog or open a Swiss bank account. What's the best alternative? It depends on the amount—and the security service that will hunt you. If you sold some commercial software programs for $50,000, it might be safe to spend the cash slowly over a couple of years. If you sold secret U.S. Government data for a million dollars, take very little cash and try to wash it through an offshore business deal in a Grand Cayman or BVI bank with a secret account. Do not keep documents about this account anywhere near you. Such an account may not be safe from FBI scrutiny, but at least the bank will not provide evidence against you in court.

CHAPTER SIX: THE WEAKEST LINK

A basic principle in the espionage business is compartmentalization, which is related to need to know. In the CIA or KGB all officers are not aware of all operations—only those in which they have a need to know. This enhances the concept of compartmentalization, which means if things go wrong in one compartment it does not spill over to other compartments.

Now ask yourself, Does my partner (spouse/girlfriend/boyfriend) really have a need to know about my secret project? Does he/she actively participate and take risks? Does my partner need to be exposed to what I'm doing? How would they behave if law enforcement officials questioned them for days on end? And finally, ask yourself, "What if years or months from now, he/she doesn't love me anymore and, further, has become quite upset with me?

I can't tell you from my experience and readings how many espionage cases have been broken due to a partner that talked. There have been many on both sides. Sometimes the partner even tipped off the police. Think of John Walker, the Navy spy of the early 1980s. His ex-wife tipped off the cops. Other spy wives, such as Rosario Ames, sang like birds when interrogated to get themselves off the hook.

Why do spies tell their partners? Some because the partners are active participants in the project. Some because their partners become suspicious about sudden extra money or trips to Europe. Others, because a spy likes to brag about his/her success.

My advice is straightforward: Unless your partner is vital to the success of the project and takes equal risk, make every effort to keep your mouth shut! Explain your extra money as gambling luck. Find plausible excuses for trips to Europe. If things go wrong, you'll be glad you remained mum for two reasons:

1. Any interrogation information the police elicit will be only from your interrogation.

2. If your partner had no knowledge, he/she will not be prosecuted.

CHAPTER SEVEN: WHAT TO DO WHEN CAUGHT

My CIA training instructors at Camp Peary in the early 1980s addressed the question of getting caught by stating their famous mantra: "Deny everything, admit nothing, make counter-allegations." Simple words that express all you should think about at this critical time.

If and when this terrible moment arrives you will probably be in a state of shock. The police can make a real power show, handcuffing you in front of family and neighbors. The moment you acquiesce to their control is the moment you lose half the battle. Your mental attitude is very important at this juncture. Just think of this mantra. Don't try to analyze what went wrong, who will take care of your family, or what the neighbors will say. Your most important task at this time is to beat the rap and deal with everything else later.

Any federal criminal lawyer will tell you that espionage is one of the most difficult cases to prove in a court of law. Unless the FBI has a video of you handing secret data to a third party, or you confess, it is extremely difficult for them to get a conviction. Most of the other evidence such as bank accounts or having secret data at home does not prove to a jury that you passed secret data to a foreign power. Such circumstantial evidence smells, but it proves nothing.

That is why the authorities will press for one thing: Your confession! A confession nails your coffin. Maybe you can use it to your advantage at a later date, but should never ever be used unless it is to your advantage with the advice of good legal counsel.

The police will of course tell you that your case is hopeless, that they already possess all the evidence they need, that your partner told them everything, even that they possess photos of you passing secrets to the enemy. Remember this: The authorities will lie to gain your confession. Fight! Deny it! Don't give them the time of day! Talk only with a federal criminal lawyer! And even make some accusations against the police. Threaten a counter-suit for false arrest; if you are a minority, make an issue of that; or claim you've been set up for political reasons.

If you carefully followed some of the tips I offered earlier, the authorities will have a formidable task without your confession. Practically all the convictions for espionage in the past 25 years came either from carelessness or confession. If you were very careful, and you don't confess, you'll probably walk.