MIRROR SITE

"Spy school for the rest of us."

Frightened by reality?
Sheep please exit here

SPY & COUNTERSPY

"During times of universal deceit, telling the truth becomes a revolutionary act." – George Orwell

Updated with new material October 28th, 1998. Recent changes to our website – FBI field offices added to *Spy address book* – Hit counter reset after server problem fixed – Hibernation file caution added to *Security Software* – Formatting guidelines added to *Use a one-time pad* – New article *Handling the risks* – Numerous terms added to *Glossary* – Hard disk obliteration method added to *Uncrackable Email 2* – Information link added to *Tax resistance primer* – New tools added to *Security software*

Click here for...

Stop and ask yourself...
If America is the land of the Free, then why does it

Your source of skills for freedom...

Spy & CounterSpy is a practical course in freedom skills – including countersurveillance, antisurveillance, and underground urban activism.

If you live in the USA, the odds are one in four that you will someday become a target for surveillance and repression – by a government security service like the FBI or BATF or DEA, by an intelligence agency like the NSA or CIA or DIA, by undercover cops, or others. Being innocent is no protection against the apparatus of surveillance and repression. If you're involved with any group that wants to change the *status quo*, then you're a target for surveillance – no matter how benign your goals.

Sometimes simply being an American with an open mind and a diverse range of interests is enough to invite surveillance.

Spy school for the rest of us...

The world is full of writers who claim to know a spy – until you ask for an introduction. *Spy & CounterSpy* goes even further. It contains methods that have been field-tested and proven during a decade of forced encounters with government security services, intelligence agencies, and undercover cops.

Whether you're just trying to protect your right to be left alone – or whether you're working to change a system that you see as unfair – *Spy & CounterSpy* gives you the *know-how* you need.

Written with an insider's knowledge and an outsider's outrage...

You cannot get this information anywhere else. Period. The only other people qualified to teach you these skills are the goons themselves. But they won't. They get prison sentences – and worse – for talking.

Make no mistake about it, *Spy & CounterSpy* is the world's only open source of skills for freedom – including countersurveillance, antisurveillance, and underground urban activist tactics.

You can explore this site using the links at the left side of the screen. We suggest you start with *Bureaucrat's Toolkit* for insight into how widespread the problem is – and how it's getting worse. Then try *Uncrackable Email* for a look at how persistent you must be if you want to beat a surveillance team. Click on *FBI vehicle surveillance* for insight into how the goon squads actually operate.

It's your constitutional right to know...

The Constitution recognizes your right to protect yourself from the government's secret agencies and goon squads. The readiness of these invisible groups to deceive the public, the courts, and the

take someone in Canada to write this? Our offices are just across the border. We're 9 miles outside the FBI's reach, from where we are able to help our many American friends.

media is why this Web site was created. Our commitment was further strengthened in October 1998 by Amnesty International's stinging indictment of widespread, systematic police brutality across the USA.

The best defense against any of these threats is an informed citizen. *Anyone* who tries to tell you otherwise is *not on your side*. The First Amendment and the Fourth Amendment give you the right to read about ways to protect your privacy. (Just because you want privacy doesn't mean you're hiding anything. You put letters inside envelopes, don't you? You close the door when you shower, don't you? The problem is not *you* – the problem is the government's *thought-police*.)

A growing awareness...

If you love your country but fear your government, then *F9* is for you.

More and more citizens are beginning to quietly resist the unfriendly, unaccountable, elitist mentality that pervades government. How about you? Browse the links along the left side of this page for insight into the situation. Then click on *Free F9 Subscription* if you'd like to learn more about protecting your right to be left alone.

Some of this material involves playing the game by Big Boys' Rules, so if you're easily offended by frank talk, please stay away. *(Hey, if you're happy and you know it, clank your leg-irons.)*

How to get the most from this Web site...

This is a living Web site, constantly growing, changing, evolving. No document ever represents our final position on a topic – and we reserve the right to contradict ourselves as we continue to expose the tactics of the government's secret agencies.

After reading any of the pages at *Spy & CounterSpy*, return to this page (our home page). All of the free features at our Web site can be accessed from this page.

Our credo. What principles does *Spy & CounterSpy* support?

1. Individual privacy, yes – institutional secrecy, no.
2. Individual empowerment, yes – the unaccountable elite, no.
3. Family values, yes – government's war on the people, no.

Countersurveillance, antisurveillance, and underground urban activism are profound topics, but if you prefer instead to focus on the bigger picture, a statement of our political position is also available.

SPY & COUNTERSPY

Spy school for the rest of us.

You are not alone. Here is a count of friends who have visited us. They are activists, concerned citizens, advocacy groups, dissidents, patriots, minorities, journalists – people who believe in the US Constitution and what it stands for – freedom and fairness. Between 450 and 900 of our friends visit us each day representing 90 countries. Thank you for your support.

WiseCat Hot Site Award – one of the Top 100 Web Sites.

Here is the small print. It appears here because we have found that maintaining a corporate front is the only way we can protect ourselves against interference by governments and their agencies. The legal underpinnings of our corporate front are our first line of defense against audit-attacks and other methods that the authorities use to suppress legitimate dissent, protest, and activism. The authorities are also determined to prove their hypothesis that *Spy & CounterSpy* is somehow funded by a foreign intelligence agency or terrorist group – but our double entry accounting record of corporate revenue and expenses is our shield against fabricated evidence by an overzealous investigator or case officer.

 Published by Lee Adams Seminars. Provided for research, education, information, and entertainment purposes only. We are not security consultants – we are investigative journalists and survivors of surveillance. *Spy & CounterSpy* and *Spy school for the rest of us* and *How To Make People Say Yes!* are trade-marks in USA, Canada, and/or other countries. Lee Adams Seminars is a division of Here's-how, Right-now! Seminars Inc.

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com
WEB SITE: http://www.SPYCOUNTERSPY.com

License and Limited Warranty

Spy & CounterSpy is an electronic magazine, hereinafter together with the information contained therein called the "product". By using the product you agree to the following terms and conditions. If you do not wish to be bound by these terms and conditions, do not use the product nor the information contained therein.

Spy & CounterSpy is published for information, education, entertainment and research purposes only. We are not security consultants – we are investigative journalists and survivors of surveillance. We are not rendering legal, accounting, management, security, tactical, political, or psychological counseling. If such advice is required the services of a competent professional should be obtained. We assume no responsibility for the accuracy of, or errors or omissions in, the information provided. In no event shall we be liable for any direct, indirect, consequential, special, or incidental damages arising out of the use of, or the inability to use, information described in the product. The names of persons, characters, corporations, institutions, organizations, geographic locations, products, and services used to explain and illustrate human behavior are entirely fictitious, except for the names of existing intelligence agencies, security services, and police agencies – or except as otherwise noted. No resemblance to actual individuals or entities is otherwise intended or implied.

License – *Here's-how, Right-now! Seminars Inc.* grants you, and you accept, a nonexclusive nontransferable license as follows for the product. You may use the product for your own use. You may make copies of the product on your hard disk and on floppy disk for backup purposes. You may print paper copies of the product for personal use. You may copy and distribute Internet-readable copies of the product by email, by link, by posting at your website, and for critical reviews and news reports in electronic or print form. You shall not otherwise modify or adapt the product using any means, electronic or mechanical, either in displayable form or as HTML source code. You shall not otherwise sell or transfer reproductions of the product to other parties in any way, nor rent, lease, or preview the product to other parties without the prior written permission of *Here's-how, Right-now! Seminars Inc.*

Limited Warranty – You expressly acknowledge and agree that use of the product is at your sole risk. The product is provided "as is" and without warranty of any kind, and *Here's-how, Right-now! Seminars Inc.* expressly disclaims all warranties, express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. No advertising, description, or representation, whether made by *Here's-how, Right-now! Seminars Inc.*'s agent, dealer, or employee shall be binding upon *Here's-how, Right-now! Seminars Inc.* or shall change the terms of this disclaimer or the limited warranty set forth herein. *Here's-how, Right-now! Seminars Inc.* does not warrant that the methods contained in the product will meet your requirements, or that the performance of the methods will be error-free, or that delivery of the product will be uninterrupted or error-free, or that defects in the product will be corrected. Furthermore, *Here's-how, Right-now! Seminars Inc.* does not warrant or make any representations regarding the use or the results of the use of the product in terms of its correctness, accuracy, reliability, or otherwise. No oral or written information or advice given by *Here's-how, Right-now! Seminars Inc.* or its authorized representatives shall create a warranty or in any way increase the scope of this limited warranty. Should the product prove defective, you (and not *Here's-how, Right-now! Seminars Inc.*) assume the entire cost of all necessary correction, repair, treatment, or servicing. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. *Here's-how, Right-now! Seminars Inc.* shall not be liable for special, incidental, consequential, or other damages, even if *Here's-how, Right-now! Seminars Inc.* is advised of or aware of the possibility of such damages. This means that *Here's-how, Right-now! Seminars Inc.* shall not be responsible or liable for lost profits or revenues, or for personal injury, or for damages or costs incurred as a result of loss of time, data, or use of the product, or from any other cause. In no event shall *Here's-how, Right-now! Seminars Inc.*'s liability exceed the purchase price, if any, of the product. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. The author and publisher of the product have used their best efforts in preparing the product and the material contained in it. These efforts include the research, development, and testing of the theories and methods in order to determine their effectiveness. The author and publisher make no warranty of any kind, express or implied, with regard to the techniques contained in the product. The author and publisher shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of the techniques, associated instructions, and/or claims of productivity gains.

Learning the basics...

SPY & COUNTERSPY

The FBI is not just a police agency. It is more than that. It is a security service. There are important differences between police agencies and security services.

Every government has a security service. The mission of a security service is to suppress anti-government activity. That's because the prime directive of a government is to stay in power. This means that most governments see their own population as the most serious threat.

That's where the security service comes in. This means suppressing dissent and criticism. It means preserving the status quo. It means keeping the government in power, no matter whether the government rules with the consent of the people or without the consent of the people.

Look around you. It is a self-evident truth that the nastier the government, the nastier its security service. Referring to a security service as *The Thought Police* is not too far from the truth.

The FBI understandably does not have a history of respect for civil rights in its capacity as a security service. The FBI's record of unconstitutional and illegal actions against American citizens is readily available to anyone who takes the trouble to investigate.

But don't overlook the bigger picture. The FBI is not out of control. On the contrary, it is very much in control. The FBI is acting with the knowledge – and approval – of the government. The FBI is, after all, the government's security service. The FBI is responsible for protecting the government from the people.

The people, alas, have no such protection from the government.

Until now.

What's really happening here...

The goal of this Web site is to level the playing field by providing skills to supporters of freedom and fairness.

The goal of this Web site – and the purpose of *Spy & CounterSpy* – is to level the playing field. Our mission is to provide knowledge and skills to people who support freedom and fairness. Our goal is to empower people. What does this mean? In theory, it means showing people how to protect themselves against government tyranny. In practice, it means teaching people countersurveillance skills.

Who needs countersurveillance skills? Anyone who is concerned about freedom and fundamental fairness. This means activists, dissidents, civil rights groups, militias, patriots, journalists, religious groups, grass-roots political movements, writers, minority groups, and others.

Countersurveillance skills give you the ability to reach your goals – political or otherwise – in spite of surveillance and interference by a security service like the FBI.

If you don't have countersurveillance skills, you are not going to reach your goals. The security service is going to make sure of that. In fact, you probably won't even realize that your plans have been secretly and systematically thwarted.

It's time to wake up.

Wake-up call...

Any group that engages in discussion or action that threatens the status quo should consider forming a countersurveillance section.

If you're involved in any group that challenges the status quo, the security service is going to take an interest in you. No matter how benign your goals, you are seen as a potential threat to the government. Ipso facto, you become a target for surveillance by *The Thought Police*.

Being innocent is no protection against surveillance.

Spy-proof Lesson #1 – Any group that engages in discussion or actions that challenge the status quo must have a countersurveillance section. That means any group. That means you. It is not a matter of choice. It is not a matter of opinion. It is not a matter of preference. Here's why.

Your adversary is going to engage in covert actions against you. For your group to survive and reach its goals, you must defend yourself against these covert actions. It does not matter that you don't see the government as your adversary. In fact, it's irrelevant. All that matters is that the government sees you as their adversary.

If you don't grasp this fundamental principle, then your group is doomed to mediocrity. It will never reach its goals, no matter how noble. It's like trying to play professional hockey without learning how to avoid a body-check against the boards. Wake up, sissy. Just because you'd never dream of intentionally assaulting your opponent doesn't mean that he isn't planning to deliberately cripple you at his first opportunity.

It is important that you understand what this means. A security service – and this includes the FBI – plays according to *Big Boys' Rules*. This means they play for keeps and they play to win. They offer no mercy because they expect none.

Part of growing up is the realization that the world is infested with unpleasant personality types like thugs, bullies, and sociopaths. A sizable percentage of these types end up working for – you guessed it – security services.

Another part of growing up is accepting that you just can't reason with some people.

How surveillance works...

Most people don't realize that a security service will use surveillance in four different ways – for four different purposes. These are observation, infiltration, sabotage, and intimidation. All of these threats can be lethal to you and your organization.

Surveillance threat #1 – Observation. A security service uses surveillance to watch you. They find out what you're doing. They discover who your contacts, members, operatives, associates, and friends are. They learn your plans. They use your conversations as evidence when they arrest you on charges of conspiracy. Most people don't realize that *conspiracy* is the most common grounds for arrest when surveillance is involved. Yes, just *talking* about some topics can get you arrested. What about free speech? Not when *The Thought Police* are around.

Surveillance threat #2 – Infiltration. A security service uses surveillance to learn enough about you so they can infiltrate agents into your group. Infiltration is dangerous for two reasons. First, an infiltrated agent can act as an *informant*, alerting the security service to your plans and providing evidence that can be used later for arrest, coercion, or blackmail. Second, an infiltrated agent can act as an *agent-provocateur*. This is someone who pretends to enthusiastically support your cause, while in reality encouraging you to commit illegal or reckless acts that become grounds for arrest by the security service. Many groups have been tricked into illegal behavior that they otherwise would have never considered. Do not underestimate the damage that an *agent-provocateur* can do. It is a wicked game. That's why the FBI plays it.

Surveillance threat #3 – Sabotage. A security service uses surveillance to learn everything about you, your group, its goals, and its plans. They can use this information to secretly sabotage your operations. Things just seem to go wrong at the worst moment, yet you can never really pin down what the problem is.

An effective security service has a range of sabotage capabilities, ranging from *dirty tricks* to *death squads*.

Some American citizens are beginning to speculate that the FBI may operate *death squads*. They claim it is easy for an organization that operates in secret to arrange situations where murder can be camouflaged as misadventure, accident, illness, criminal activity, chance events, or suicide. How better to disable a persistent grass-roots movement than by arranging the demise of its leader via a traffic accident, mugging, or suicide?

Surveillance threat #4 – Intimidation. A security service can use surveillance to control you. It's a form of mind control. The FBI is currently enjoying success with this tactic against a number of militia and patriot groups. That's because fear is a powerful tool. If you know you're under surveillance, you're afraid to do anything. The FBI has developed this mind-game to a sophisticated level. After they've let you see their surveillance team, they merely need to make an appearance once a month or so. You're so terrified that you assume you're under surveillance 24-hours a day. The FBI has won. You are paralyzed by fear. For some targets of surveillance, all that's required is an appearance twice a year by the FBI to keep you immobilized. Of course, none of these mind-games work if you've got countersurveillance skills and can spot the gaps in surveillance.

How countersurveillance works...

Most people don't realize what countersurveillance can achieve for them. First, it gives you the ability to detect the presence of a surveillance team. This means you can immediately stop engaging in any behavior that might incriminate you. But, even more important, countersurveillance skills can give you the ability to cloak your actions. You can carry out operations without the knowledge of the surveillance team. This means your group can reach its goals even while under hostile surveillance.

Countersurveillance advantage #1 – Detecting your adversary. If you can detect the presence of the surveillance team, you can avoid arrest by immediately stopping any activity that might incriminate you. Being able to detect surveillance gives you a margin of safety that you otherwise wouldn't have.

Countersurveillance advantage #2 – Thwarting your adversary. Knowing that you're under surveillance means you can begin to thwart your adversary's attempts to gather information about you. For example, realizing that your vehicle is bugged means that you'll stop engaging in incriminating conversation in your car. Or, even better, you can engage in contrived conversations and feed misinformation to the surveillance team. Being able to detect surveillance gives you the opportunity to confuse and confound the security service.

Countersurveillance advantage #3 – Achieving your goals. Detecting surveillance and thwarting the surveillance team are noteworthy achievements. They enable you and your group to survive. But they're strictly defensive. You'll never achieve your goals until you go on the offensive. And that's the most powerful benefit that countersurveillance can give you – the ability to keep doing what you want to, even though you're under surveillance.

Around the world, a number of intelligence agencies and guerrilla groups have proven that you can carry out operations while you're under hostile surveillance – and the security service will be none the wiser.

These intelligence agencies and guerrilla groups have developed a system for surviving – *and thriving* – while under surveillance. A number of underground groups are already using this system to conduct operations in the United States.

Here's why it works. A security service can only achieve its objectives by intercepting communication between people. This means you can beat the security service if you can deny them the ability to watch, read, overhear, or participate in your communication with other people. In effect, you can beat the security service by using *stealth*. You can do this in two ways.

***Stealth* method #1** – If you are skilled in countersurveillance, you can exploit the gaps that are present in surveillance operations. This means you engage in operational activity only when the surveillance team isn't monitoring you. Even round-the-clock surveillance has gaps in it. If you're under sporadic FBI surveillance designed to intimidate you by keeping you frightened, you'll enjoy huge gaps that you can exploit.

***Stealth* method #2** – If you are skilled in elliptical conversation, you can carry on communications even though you're under surveillance. Elliptical conversation is dialog that says one thing but means another. Quite often two people who've known each other for a long time have built up a kind of shorthand conversation. By referring to past shared incidents that the surveillance team is unaware of, the two individuals can send hidden meanings to one another. They can also use code-words to disguise the real meaning of their communication.

Where do you go from here?

If you are involved in a group or enterprise that is attempting to change the status quo, you must accept that countersurveillance needs to be a part of your planning and operations. The keys to success are twofold – knowledge and skills. First, you need knowledge of your adversary's capabilities. Second, you need skills in the art of countersurveillance. You can get both by reading *Spy & CounterSpy*. In fact, that's the only way you can get them.

SPY & COUNTERSPY

Spy school for the rest of us.

Back to Home Page

Here is the small print. It appears here because we have found that maintaining a corporate front is the only way we can protect ourselves against interference by governments and their agencies. The legal underpinnings of our corporate front are our first line of defense against audit-attacks and other methods of economic warfare that the authorities use to suppress dissent, protest, and activism. They are also determined to prove their hypothesis that *Spy & CounterSpy* is funded by a foreign intelligence agency or terrorist group – but our double entry accounting record of corporate revenue and expenses is our shield against fabricated evidence by an overzealous investigator or case officer.

Lee Adams Seminars is a division of Here's-how, Right-now! Seminars Inc.
OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com
EMAIL ENCRYPTION: Click on *Ask Agent X* for our public key.

Too good to be true?

Maybe you've looked through the *Spy & CounterSpy* Web site and now you're thinking to yourself, Gee, this is too good to be true.

An attitude like that shows common sense. It's smart to be skeptical. Being skeptical is one of the first things you learn in countersurveillance. Take nothing for granted. Take nothing at face value. And that includes the *Spy & CounterSpy* Web site.

We don't mind being held up for close inspection. Keep reading and we'll explain how you can test us and prove to yourself that we're not an *agent-provocateur* for the FBI.

Yes, it's okay to be cautious, even a bit suspicious. But you don't want your choices to become limited by fear. You don't want to let fear run your life.

And it can easily happen. Here's why.

The urban setting. Surveillance often occurs in an urban setting. Offices. Homes. Streets. Sidewalks. Motels. Restaurants. Neighborhoods.

Surveillance is urban conflict. It's that simple. As soon as you become aware you're being watched, surveillance becomes urban conflict.

A number of governments have done research into urban conflict. Why? Because governments create urban conflict with their security service, undercover cops, and other operations. They do research so they can understand how to fully control the urban conflict they create. (Example: intelligence units of US Marines are currently mapping *Chicago*.)

Urban conflict is stressful. Extremely stressful. Here's how it affects the people who are involved. In this discussion we'll refer to them as combatants.

75% of combatants in urban conflicts suffer from an affective disorder. That's *shrink-talk* for your mood – you're stressed-out, high-strung, on edge. It also includes measureable things like an exaggerated startle reflex, as well as your ability to concentrate and stay focused.

25% of combatants suffer something more serious called a neurotic disorder. That's *shrink-talk* for anxiety. You're being really cautious, really suspicious – a bit paranoid.

And, finally, nearly 10% of combatants have a psychotic episode – forget the *shrink-talk* for these folks, they're just plain gone.

The conclusion? Urban conflict is very stress-inducing for people like cops, narcs, SWAT teams, riot squads, informants, you know the type. It's also stressful for surveillance teams – and for the targets of surveillance. That means people like you and me. This is just part of the unavoidable damage a surveillance team inflicts on you, no matter whether you're guilty or innocent.

Here's what you need to do. First, remember that you're not alone. All targets of surveillance go through this. It's natural. It's part of the game.

You need to be careful not to fall into the trap of being too suspicious, too cautious. You've got to be careful to avoid becoming one of the 25% who let fear run their lives. Even falling into the 75% category can significantly degrade your ability to function under surveillance.

The best way to avoid this? Think things through. Logically. Sensibly.

Of course the FBI doesn't want you to do that. The FBI would prefer you let fear make your decisions. Don't let the FBI win that head-game.

Thinking it through...

There are three factors that affect you and the *Spy & CounterSpy* Web site. You should think them through. These

three factors are lawfulness, dataveillance, and openness. The good news is – you're in the clear in all three of these factors.

Lawfulness. This is the first factor affecting you and the *Spy & CounterSpy* Web site. It is completely legal for you to read *Spy & CounterSpy*. Even though the information is extremely sensitive, it has been compiled using accepted methods of investigative journalism. Plus, the Constitution of the United States recognizes your right to protect yourself from the government's secret agencies. So you're not doing anything wrong by being interested in surveillance and countersurveillance.

Of course, an FBI or ATF surveillance team will do their best to make you feel guilty about trying to learn more. That's because they don't want you to level the playing field. The goons prefer to have you always fighting an uphill battle. They don't want you to get smart.

Dataveillance. This is the second factor affecting you and the *Spy & CounterSpy* Web site. Dataveillance is spy-talk for using data as a surveillance tool. If you've browsed this site, you've probably already browsed other controversial sites. That means you're already on a list somewhere.

The National Security Agency routinely monitors electronic communication in the USA. Not just some of it. *All of it.* That means telephone conversations, fax transmissions, telexes, email, and the Internet. All of it. They're continually scanning for communication that might interest them. And they're very good at what they do.

The NSA has some very powerful computers. And they've come up with some clever ways of using them. They use them to search for *keywords*. They also have some powerful *voice-recognition* software. For the NSA, tracking someone on the Internet is child's play.

So don't kid yourself. If you've done any serious browsing on the Internet – or if you've ever engaged in any "interesting" telephone conversations – then your name is already on an NSA list. And the NSA shares its information with the FBI, ATF, DEA – even other countries. They've already got you pegged as someone with a *predisposition*, whatever that means.

So you're not necessarily attracting new surveillance by reading *Spy & CounterSpy*. In practical terms, you invite surveillance simply by being an American citizen with a diverse range of interests. Don't feel guilty about what you're doing – you're not the problem, the government is. They're the ones running the secret agencies who function as *thought-police* in the USA.

Openness. This is the third factor affecting you and the *Spy & CounterSpy* Web site. It simply doesn't matter if the FBI, ATF, DEA, or any other surveillance team sees you reading this stuff. They don't gain any advantage. You don't suffer any disadvantage.

Think of it this way. Reading *Spy & CounterSpy* is like reading a book about playing chess. The fact that your opponent knows you've been studying books on chess doesn't hurt you. It's irrelevant. What counts is what happens on the board.

Likewise, the fact that the FBI knows you've been reading articles about countersurveillance doesn't hurt you. It's irrelevant. What counts is what happens on the board.

Spy & CounterSpy will teach you techniques for use in specific situations that surveillance teams can't avoid. But, even more important, *Spy & CounterSpy* will teach you the concepts and principles of countersurveillance. When you understand these concepts, you'll be able to adapt to many different surveillance situations. Best of all, the FBI simply has no way of knowing how you're going to use what you've learned.

Where do you want to be?

Let logic, not fear, run your life. Think things through. Consider where you are now. Then consider where you'll be if you take advantage of the information and *know-how* available through *Spy & CounterSpy*.

Privacy is your *right*. Just because you want privacy doesn't mean you're hiding anything. *You put letters inside envelopes, don't you? You close the bathroom door when you shower, don't you?* You have a pre-existing right to privacy that is

recognized by the US Constitution.

So if you're presently engaging in behavior that you don't want the FBI to find out about – here's what you should do. Suspend your activities while you read *Spy & CounterSpy*. You'll soon see that our articles have the ring of truth to them. You'll be able to apply what you learn right away – and you'll start seeing results right away.

SECURITY NOTE – Are we an agent-provocateur? Well, we can't prove a negative. We can't prove we're *not* an agent-provocateur. But we *can* prove a positive. We *can* prove that we provide reliable, useful, hard-hitting information about countersurveillance, antisurveillance, and methods for underground urban activists. We're not asking you to take our word for it. We're asking you to try it for yourself.

Who funds us?

Spy & Counterspy is not beholden to anyone – not government, not big business, not multinational corporations, not the mainstream news media, not the military-industrial complex, and not the newly-emerging police-industrial complex.

So our articles are hard-hitting. We point fingers. We name names. We don't pull our punches. Everyone here works hard to make *Spy & CounterSpy* a trustworthy source of information about how to protect your right to be left alone.

So where do we get funding? From people just like you. From supporters who understand the value of an ongoing independent source of information about countersurveillance, antisurveillance, and methods for underground urban activists. People who understand how important it is to protect freedom against what they see as a growing threat of government tyranny.

CONTRIBUTIONS – If you would like to make a contribution, please make your check, money order, or bank draft payable to *Here's-how, Right-now! Seminars Inc.* and mail it to PO Box 8026, Victoria BC V8W 3R7 Canada or send it by courier to 3273 Tennyson Avenue in Victoria. If you prefer to use your credit card, call Vickie at 250-475-1450.

We are grateful for this support, because it helps us keep up our corporate front. The corporate veil is one of our defense mechanisms against the goons.

SPY & COUNTERSPY

Spy school for the rest of us.

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com

Vehicle surveillance: The FBI's system...

Part one in a five-part series

Wheel artist – that's spy-talk for an outdoor surveillance specialist operating in a vehicle. The FBI has lots of them – agents and bucars (bureau cars). Together they're called *vehicle surveillance teams*.

Know your adversary. Make no mistake about it, FBI vehicle surveillance teams are *deadly*. They get results. Consistently. FBI agents receive the best training and the best equipment.

They don't just follow you – they *surround* you. They become part of your environment. You never see the same vehicle twice. They blend in with traffic. Up to twenty FBI agents at any one time. Even more if the investigation involves national security.

Every agent on the surveillance team has just one thing on his mind – *to get you*. And they will.

Unless you read this article. Carefully.

What you'll learn

This is the first article in a *five-part series* that teaches you how to respond when you're confronted by an FBI vehicle surveillance team.

Article #1 – In the first tutorial (the article you're reading now) you'll learn the fundamentals of how vehicle surveillance teams operate.

Article #2 – In the second tutorial you'll learn about the tactics, diversions, and decoys that an FBI surveillance team uses – including how they support the foot surveillance team.

Article #3 – In the third tutorial you'll learn about advanced methods like setups, traps, ambushes, and attacks – as well as the FBI's psychological operations against you while you're driving.

Article #4 – In the fourth tutorial you'll see how to use *antisurveillance* and *countersurveillance*. You'll learn how to detect and obstruct the FBI.

Article #5 – In the fifth and final article you'll receive *step-by-step instructions* for breaking out of FBI surveillance. You'll learn how to give them the slip.

How you'll benefit. This five-part series of articles provides *practical training* in professional countersurveillance and antisurveillance techniques. If you are the target of FBI surveillance, this article will give you the edge you need to outwit the goon squads of government tyranny and repression.

The FBI: A dangerous adversary...

The FBI is mainly interested in activity that occurs while you are out of your vehicle. The goal of an FBI vehicle surveillance team, therefore, is to track you to that location – and then help the foot surveillance team establish contact on you.

Background. The FBI's vehicle surveillance system is the result of six decades of experience. From rudimentary beginnings during Prohibition, the FBI system as it exists today is built in large part from techniques originally developed from 1938 to 1943 by the Gestapo to monitor and suppress resistance in Nazi-occupied countries. With the addition of more than 50 years of modifications and improvements, the FBI today possesses a surveillance apparatus that has led to the ruin of many suspects.

Triple threat

Depending on the situation, FBI agents can choose from three different methods of vehicle surveillance. These methods are

floating-box surveillance, *hand-off* surveillance, and *static* surveillance.

Floating-box surveillance. Floating-box surveillance is based on continuous coverage by the same team. FBI agents create a box of surveillance vehicles around you. The box floats with you as you travel along your route. Hence the name floating-box. It is very effective in urban and suburban locations. Very few suspects break out of a properly-run floating-box.

Hand-off surveillance. Hand-off surveillance involves more than one team. At key intersections or other *decision points* along your route, surveillance control is passed from one floating-box team to another. This is called phased coverage. It is very effective when large distances are involved – freeways, expressways, long commutes, highways, and so on. It is also used in city situations when lengthy periods of time are involved.

Static surveillance. Static surveillance is also based on phased coverage, but it uses*fixed observation posts* instead of a floating-box. Each observation post is located at a decision point (major intersection, etc.) along the target's route. Although this method of surveillance leaves many gaps in coverage, it is very difficult to detect this type of surveillance. The FBI uses this method when they first begin coverage on a hard target (such as a trained intelligence agent who is likely to be on the lookout for surveillance). The FBI swtiches to floating-box surveillance after they have identified general locations where coverage is required.

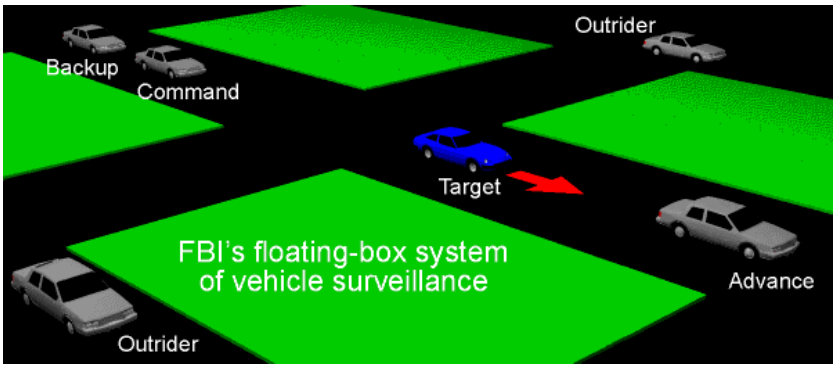
The FBI's floating box system...

The FBI's floating-box is a powerful system. The wheel artists don't follow you – they *surround* you. They blend in. They become part of your ecosystem.

An FBI floating-box can be run with as few as three vehicles – or as many as 20. A team consisting of seven to ten vehicles is typical. It is not unheard-of for 50 vehicles to be involved, especially in a major case where arrest is imminent.

The FBI has for many years managed to keep secret the size of their vehicle surveillance teams. Even in court proceedings, the most they'll admit to is 20 vehicles. In some surveillance situations, FBI wheel artists don't just blend in with your environment, they *become* your environment.

The image shown below illustrates the major components of the FBI's*floating-box* system of vehicle surveillance.



The target's vehicle is shown in blue. The vehicles of the surveillance team are depicted in gray. The green rectangles represent urban terrain.

The illustration is not rendered to scale. Distances in the real world are significantly greater. Furthermore, surveillance vehicles in the real world are *never* the identical make, model, and color. FBI teams use sedans, coupes, stationwagons, pickup trucks, vans, minivans, sport utility vehicles, taxis, motorcycles, commercial trucks, ambulances, 18-wheelers, and others.

Specialized roles

Each of the surveillance vehicles in the above illustration is charged with carrying out a specific assignment.

Command vehicle. The *command vehicle* is tasked with maintaining visual contact with the target. The agent is said to have *command of the target*. This is a pivotal role. This agent keeps the

command of the target. This is a pivotal role. This agent keeps the other team members informed of the target's direction, speed, intentions, etc.

Backup vehicle. The *backup vehicle* provides a fill-in function. Because the *command vehicle* is the vehicle most likely to be detected by the target, the FBI has devised a number of strategies that let the *backup vehicle* take over the command role, thereby allowing the previous command vehicle to exit the surveillance box. Many suspects have been duped by this strategy, as you'll learn later in this article.

Advance vehicle. The *advance vehicle* is like an early warning system. The agent provides advance warning of obstacles, hazards, or traffic conditions that would otherwise catch the surveillance team unaware. The *advance vehicle* also fulfills another important function. If the FBI has bugged your telephone or your office or your residence, they're likely to already know your destination. Naturally, the *advance vehicle* arrives before you do. Many suspects have been completely fooled by the undercover FBI agent who is already seated at the restaurant when the suspect arrives.

Outrider vehicle. The *outrider vehicles* patrol the perimeter of the floating-box. Their assignment is to make certain that the target does not get outside the containment of the box. They also play a key role when the target makes a turn at an intersection, as you'll learn later in this article.

Surveillance advantages

The floating-box is a very powerful and flexible system. It allows the FBI to successfully respond to a variety of situations. The FBI is almost never caught off-guard.

Recovery from mistakes. If visual contact with the target is lost, the box can be collapsed inward, enabling the agents to quickly re-acquire *command of the target*. (Whenever the FBI loses visual contact with the target, the surveillance team immediately executes a *lost-command drill*. The FBI has a number of strategies they use to re-acquire *command of the target*.)

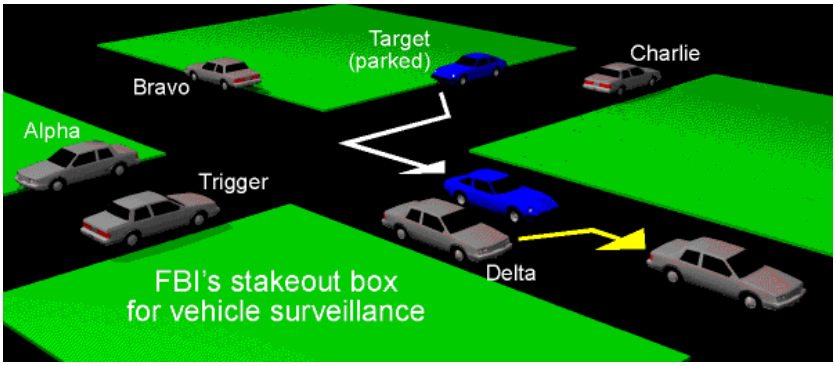
Quick response. The floating-box also allows the FBI to react quickly to a target who is attempting to evade surveillance. If the target unexpectedly makes a left turn, for example, the left *outrider vehicle* turns left and becomes the new *advance vehicle*. The other elements in the team shift roles as appropriate. More on this later.

Signature shift. The floating-box makes it possible to quickly alter the signature of the team, making them more difficult to detect. In the previous illustration of the floating-box system, there are five surveillance vehicles. At first glance one might assume they can be reconfigured five different ways if they switch roles. In actual practise, a team of five vehicles can be reconfigured 5x4x3x2x1 = 120 different ways. Not all of these configurations are useful in the field, especially when the command vehicle's role is unchanged. In practise, about two dozen configurations are practical – more than enough to deceive most targets.

The FBI's stakeout box...

A vehicle surveillance operation begins with a *stakeout box*. The FBI watches your office or residence, waiting for you to get in your vehicle and drive away. At that moment the *stakeout box* becomes a*floating-box*.

The image shown below illustrates the basic components of an FBI stakeout box.



The target's vehicle is shown in blue. The vehicles of the surveillance team are depicted in gray. The image is not rendered to scale. Distances are much greater in the real world.

Assignments

Note how vehicles Alpha, Brava, Charlie, and Delta are prepositioned. They are pointed away from the parked *target vehicle*. Each of these four *layup vehicles* is ready to initiate a *follow*, no matter which direction the target takes.

Trigger vehicle. The *trigger vehicle* is responsible for maintaining visual contact with the parked *target vehicle*. When the target begins to drive away, the agent in the *trigger vehicle* alerts the other members of the *stakeout box*. The agent is triggering the rest of the team into action – hence the name, *trigger vehicle*.

Layup vehicle. After being alerted by the *trigger vehicle*, the appropriate *layup vehicle* – Alpha, Bravo, Charlie, or Delta – picks up the *follow* and becomes the *command vehicle*. The other vehicles assume roles as *outriders* and *backup* until the team can be augmented with other FBI vehicles being held in reserve.

Picking up the follow. In a smoothly-run stakeout box, the *layup vehicle* that is initiating the *follow* will often pull out in front of the target vehicle, as shown in the illustration above. The layup vehicle becomes the *command vehicle*, with *command of the target*. When the command vehicle is in front of the moving target vehicle, it is called *cheating*. A *cheating command vehicle* is more difficult to detect that a command vehicle that is following the target.

Command of the target...

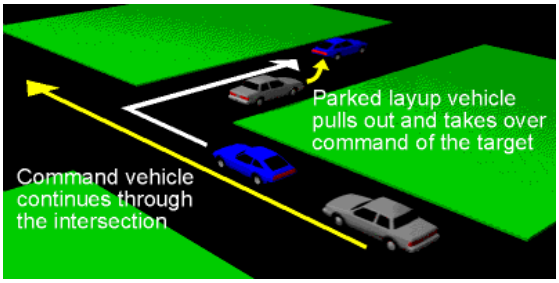
The phrase *command of the target* refers to visual contact with the target of the surveillance operation. The surveillance vehicle having command of the target is called the *command vehicle*.

The name is appropriate, for the command vehicle also has virtual command of the entire surveillance team. The agent in the command vehicle informs the rest of the team whenever the target vehicle changes direction, adjusts speed, or stops. The surveillance team follows the guidance of the command vehicle.

The control and power that is provided by this approach is offset by the *vulnerability* of the command vehicle. In many surveillance operations, it is the command vehicle that is first detected by the target. In order to overcome this vulnerability, the FBI has developed a number of tactics to dupe the target of the surveillance operation.

Hand-off. The image shown below provides an example of how the FBI often reacts to a turn by the target vehicle.

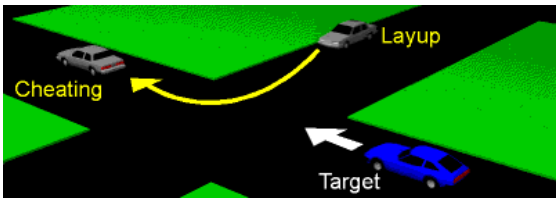
SPY & COUNTERSPY



After watching the target make a right turn at the intersection, the *command vehicle* continues straight through the intersection. The agent has, however, alerted one of the *layup vehicles* that the FBI has prepositioned at major *decision points* along the target's route.

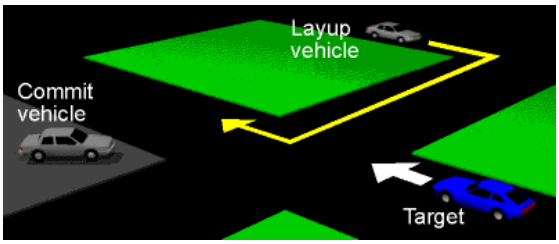
As you can see from the illustration above, this is a very potent maneuver. The target sees the car that has been following him continue straight through the intersection. He starts to question whether or not he was actually under surveillance – perhaps he was just "imagining things". As a result, the *layup vehicle* is often able to pick up *the follow* without attracting any suspicion.

Cheating. The image shown below shows a variation on this maneuver. Instead of pulling in behind the target, the *layup vehicle* acquires *command of the target* by pulling out ahead of the target. This is called a *cheating* command. It has fooled a lot of suspects of FBI investigations.



A *hard target*, however, will eventually notice a *telltale pattern* of vehicles on side streets who pull away from the curb and turn the corner in front of him. (This is how you detect surveillance teams – by watching for patterns of behavior around you.)

Commit vehicle. In order to further disguise their activities, the FBI often utilizes a *commit vehicle*, as shown in the illustration below.



The *commit vehicle* is prepositioned at a major *decision point* along the target's route. The FBI agent in the commit vehicle is charged with watching the approaching target vehicle. His assignment is to observe when the target has committed himself to a specific route. Hence the name *commit vehicle*. Because he is parked in a parking lot, driveway, or side street, his presence is difficult to detect by the target.

Using a tactic like this allows the *layup vehicle* to be parked out of sight, as shown in the image above.

At the appropriate moment the *commit vehicle* cues the *layup vehicle* to begin moving. This permits the layup vehicle to smoothly enter the situation and acquire *command of the target* without attracting the attention of the target. The target does not see the layup vehicle pull away from the curb – he only sees what appears to be just another vehicle in the normal flow of traffic.

BACKGROUND – A significant portion of the FBI's training program is devoted to timing. Agents must become proficient at judging distance and time during surveillance operations. If the agent in the *commit vehicle* does her job properly, she can cue the *layup vehicle* to enter the situation in a manner that is invisible to the target. FBI recruits spend weeks learning these skills – and an entire career perfecting them. The FBI denies that Seattle, Atlanta, New York, and Philadelphia are key training areas for their vehicle surveillance teams.

End of article #1

Coming up in Article #2...

In the next tutorial in this five-part series you'll learn about the tactics, diversions, and decoys that an FBI vehicle surveillance team uses to keep you from detecting them. You'll see how the FBI modifies its vehicles. You'll find out about the basic driving skills of FBI *wheel artists*. You'll learn why you never see them communicating with each other. You'll see how the vehicle surveillance team supports the foot surveillance team.

Coming up in Article #3...

In the third tutorial you'll learn about advanced methods of vehicle surveillance, like setups, traps, ambushes, and attacks. You'll also find out about psychological operations that the FBI can run against you while you're driving. You'll discover how they can use operant conditioning to covertly coerce you to alter your route – and leave you thinking it was *your* idea. Case studies supported by *custom-prepared* illustrations show you exactly how it's done.

Coming up in Article #4...

In the fourth tutorial you'll learn how to defend yourself against a vehicle surveillance team. You'll find out about *antisurveillance* – that's spy-talk for detecting the presence of vehicle surveillance.

You'll learn about the telltale patterns that give them away. You'll be able to detect them *without them realizing you've spotted them*. You'll see five maneuvers you can use while driving to trick them into revealing themselves.

You'll also learn about *countersurveillance* – that's spy-talk for obstructing and harassing a vehicle surveillance team. You'll see ten maneuvers you can use while driving to make things *very unpleasant* for the FBI.

Coming up in Article #5...

In the fifth tutorial you'll receive *step-by-step instructions* for breaking out of surveillance. You'll see how to give the goons the slip. You'll learn three methods for exploiting the flaws in the FBI's *floating-box* system.

The first method teaches you how to out-maneuver a *cheating command* vehicle and its backup unit. The second method shows you how to beat the FBI's *stakeout box*. The third method explains how to slip away while the goons are shifting from vehicle to foot surveillance.

In each case the FBI is forced to implement a *lost-command drill* in order to try and find you again.

How to make certain you get all the tutorials...

The next article is scheduled for publication in mid-September. There are three ways you can ensure you don't miss any of the articles.

1. Visit our site regularly. *Spy & CounterSpy* is a living Web site, constantly growing, changing, evolving. We are involved in a continuing struggle to expose the tactics of the government's secret agencies. Return to our home page and bookmark our site. Visit us weekly – and you'll be assured of keeping up with the latest developments.

2. Become a member of *F9*. Return to our home page and click on *Free F9 membership*. In addition to receiving the free *F9* weekly bulletin, you'll receive email notification whenever a new article is posted at our Web site.

3. Get on our contact list. Simply click here to send email asking Vickie to add your name and your email address to our contact list. We'll email you whenever we issue a news release or

contact list. We'll email you whenever we issue a news release or publish a new article at our Web site.

NOTE – If you're concerned about your personal privacy, please consider using a cyber-cafe and a *nom de guerre* with an anonymous free email account.

Spy school for the rest of us.

http://www.SPYCOUNTERSPY.com

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com
WEB SITE: http://www.SPYCOUNTERSPY.com

License and Limited Warranty

Spy & CounterSpy is an electronic magazine, hereinafter together with the information contained therein called the "product". By using the product you agree to the following terms and conditions. If you do not wish to be bound by these terms and conditions, do not use the product nor the information contained therein.

Spy & CounterSpy is published for information, education, entertainment and research purposes only. We are not security consultants – we are investigative journalists and survivors of surveillance. We are not rendering legal, accounting, management, security, tactical, political, or psychological counseling. If such advice is required the services of a competent professional should be obtained. We assume no responsibility for the accuracy of, or errors or omissions in, the information provided. In no event shall we be liable for any direct, indirect, consequential, special, or incidental damages arising out of the use of, or the inability to use, information described in the product. The names of persons, characters, corporations, institutions, organizations, geographic locations, products, and services used to explain and illustrate human behavior are entirely fictitious, except for the names of existing intelligence agencies, security services, and police agencies – or except as otherwise noted. No resemblance to actual individuals or entities is otherwise intended or implied.

License – *Here's-how, Right-now! Seminars Inc.* grants you, and you accept, a nonexclusive nontransferable license as follows for the product. You may use the product for your own use. You may make copies of the product on your hard disk and on floppy disk for backup purposes. You may print paper copies of the product for personal use. You may copy and distribute Internet-readable copies of the product by email, by link, by posting at your website, and for critical reviews and news reports in electronic or print form. You shall not otherwise modify or adapt the product using any means, electronic or mechanical, either in displayable form or as HTML source code. You shall not otherwise sell or transfer reproductions of the product to other parties in any way, nor rent, lease, or preview the product to other parties without the prior written permission of *Here's-how, Right-now! Seminars Inc.*

Limited Warranty – You expressly acknowledge and agree that use of the product is at your sole risk. The product is provided "as is" and without warranty of any kind, and *Here's-how, Right-now! Seminars Inc.* expressly disclaims all warranties, express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. No advertising, description, or representation, whether made by *Here's-how, Right-now! Seminars Inc.*'s agent, dealer, or employee shall be binding upon *Here's-how, Right-now! Seminars Inc.* or shall change the terms of this disclaimer or the limited warranty set forth herein. *Here's-how, Right-now! Seminars Inc.* does not warrant that the methods contained in the product will meet your requirements, or that the performance of the methods will be error-free, or that delivery of the product will be uninterrupted or error-free, or that defects in the product will be corrected. Furthermore, *Here's-how, Right-now! Seminars Inc.* does not warrant or make any representations regarding the use or the results of the use of the product in terms of its correctness, accuracy, reliability, or otherwise. No oral or written information or advice given by *Here's-how, Right-now! Seminars Inc.* or its authorized representatives shall create a warranty or in any way increase the scope of this limited warranty. Should the product prove defective, you (and not *Here's-how, Right-now! Seminars Inc.*) assume the entire cost of all necessary correction, repair, treatment, or servicing. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. *Here's-how, Right-now! Seminars Inc.* shall not be liable for special, incidental, consequential, or other damages, even if *Here's-how, Right-now! Seminars Inc.* is advised of or aware of the possibility of such damages. This means that *Here's-how, Right-now! Seminars Inc.* shall not be responsible or liable for lost profits or revenues, or for personal injury, or for damages or costs incurred as a result of loss of time, data, or use of the product, or from any other cause. In no event shall *Here's-how, Right-now! Seminars Inc.*'s liability exceed the purchase price, if any, of the product. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. The author and publisher of the product have used their best efforts in preparing the product and the material contained in it. These efforts include the research, development, and testing of the theories and methods in order to determine their effectiveness. The author and publisher make no warranty of any kind, express or implied, with regard to the techniques contained in the product. The author and publisher shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of the techniques, associated instructions, and/or claims of productivity gains.

Vehicle surveillance: Basic tactics of the FBI...

This is the second article in a five-part series that teaches you how to respond when confronted by FBI *wheel artists* – and the FBI's floating-box system of vehicle surveillance.

If you haven't yet read the first article, please return to our home page and click on *FBI vehicle surveillance 1*.

The story up to now. In the previous article you learned about the FBI's floating-box system. You saw how FBI agents don't just follow you, they *surround* you.

You also found out about the different functions of each vehicle in the surveillance team – command, backup, outriders, and advance. You also discovered how the FBI's *stakeout box* operates. You learned how the *trigger* vehicle signals the *layup* vehicle to pick up the *follow* when the target drives away.

Even more important, you learned about *command of the target*. You saw how a *cheating* command vehicle is located in front of the target. You learned how a *commit* vehicle is located at a *decision point*. You saw how the commit vehicle is used to cue a *layup* vehicle to enter the situation and assume command of the target.

What you'll learn next. In this tutorial you'll learn about the mechanical modifications that the FBI makes to its surveillance vehicles. You'll see how these modifications give the surveillance team an advantage over you.

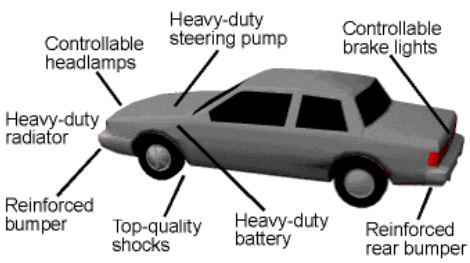
You'll also see how the members of the surveillance team communicate with each other. You'll learn why you never see them talking.

You'll see graphic examples of teamwork and tactics utilized by the surveillance team. You'll learn how they handle intersection turns, U-turns, returning to a parked car, and other situations. You'll also discover how the *vehicle* surveillance team supports the activities of the *foot* surveillance team.

Vehicle modifications...

The FBI employs a potpourri of different vehicles in its surveillance operations. *Wheel artists* drive anything and everything, including sedans, coupes, stationwagons, pickup trucks, vans, minivans, sport utility vehicles, taxis, motorcycles, commercial trucks, ambulances, 18-wheelers, and others.

Many of these surveillance vehicles have been specially modified for their role. See the illustration below.



Probably the most significant modification is the addition of cutout switches and dimmer switches for many of the lights on the surveillance vehicle.

Headlamps. The driver can disable either of the front headlamps. He can also adjust the brightness of the headlamps. This provides a tremendous advantage at night – the agent can alter the way her vehicle appears to other drivers. For part of the *follow* the

surveillance vehicle has two normal headlamps. For a while it might show only the left headlamp. And for part of the *follow* the vehicle might exhibit dimmed headlamps, suggestive of a faulty alternator or low battery condition. Many unwitting targets of surveillance have been completely hoodwinked by this feature.

Brake lights. The FBI agent can also disable the vehicle's brake lights. This is particularly effective when the agent has a *cheating command* of the target. That means the FBI agent is positioned ahead of the target. If the agent's brake lights are not continually flashing, the target is less likely to detect that the agent is adjusting her speed in order to maintain a constant distance in front of the target. Again, many targets have been fooled by this modification.

Stall switch. Some FBI surveillance vehicles are equipped with a *stall switch*. This allows the *wheel artist* to simulate a vehicle breakdown. This deception is particularly effective in helping the FBI recover from mistakes during a *follow*. Stalled in front of the target vehicle, and apparently unable to get the vehicle restarted, an FBI agent is able to delay the target until the rest of the surveillance team gets back in position.

Bumpers. FBI surveillance vehicles can be equipped with reinforced ramming bumpers. These are effective when agents need to prevent a suspect from fleeing – or force a victim off the road at high speed.

Standard modifications. Because of the stress involved in constant on-road use, FBI mechanics routinely make a number of standard modifications to the Bureau's surveillance vehicles. They often install a heavy-duty radiator and battery. A heavy-duty steering pump is also a common feature. These, along with top-quality shocks and springs, enhance the *staying power* of the vehicle during long *follows*.

One of our contacts has recently told us that the FBI uses stainless steel brake lines in many of its surveillance vehicles. This modification apparently boosts performance by overcoming certain types of condensation and heat-related problems during some weather conditions.

Driver communications...

A typical radio transmission between FBI *wheel artists* goes something like this.

"Gamma is flipping. Possible spark or smoke."

In plain language, this means *"The target vehicle has just made a U-turn. He may have detected us."*

By using communication codes, the FBI is able to reduce the chances of an eavesdropper figuring out what's going on. Anyone picking up a stray signal is unlikely to realize that it's from a surveillance team. For examples of surveillance team communication codes, return to our home page and click on *Surveillance codes*.

Why you never see them communicating. FBI agents are trained to conceal their voice communications. Often two agents will be riding in one vehicle. In order to disguise a radio transmission, the agent in the passenger seat will turn his/her head towards the driver while transmitting. If you're stopped at a red light ahead of the FBI surveillance vehicle, all you'll see in the rear view mirror is two people who *appear* to be talking to each other.

During a surveillance operation, FBI agents can use either their body rigs or the vehicle radio sets for transmitting. The body rig includes a standalone, internally mounted ear-piece that is virtually undetectable unless you're looking for it. The effective range of the FBI's standard body rig is much less than their vehicle radio sets. Both the body-rig and the vehicle set offer hands-free operation.

CASE STUDY: Hostile situation. When an FBI agent finds herself alone in a congested traffic situation with the target – and perhaps under close visual scrutiny by a suspicious target – she can still transmit critical information to the team leader. She simply clicks her tongue instead of talking. Here's an example.

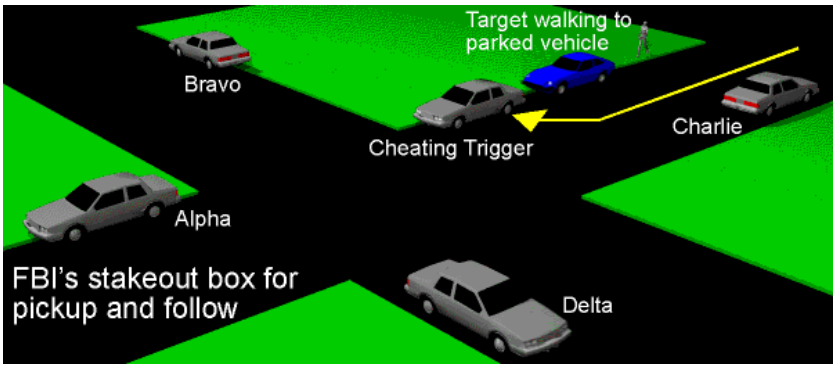
Wheel artist – numerous clicks.
Controller – "Is that you, Echo?"
Wheel artist – two clicks (*Yes*).
Controller – "Are you in command of the target?"

Wheel artist – two clicks (*Yes*).
Controller – "Has the target made contact with the other suspect yet?"
Wheel artist – silence (Possible *No*).
Controller – "Is the target *not* in contact with the suspect?"
Wheel artist – Two clicks (*Yes*).

And so it continues, two clicks meaning *Yes*, silence meaning *No*.

Real-time communication...

The FBI has found that agent-to-agent communication *in real-time* is a vital component of a productive surveillance operation. Real-time communication gives the surveillance team a tactical advantage over the target. The illustration shown below provides a good example of this principle.



As the target walks back towards his parked vehicle, the various members of the vehicle surveillance team take up positions in a standard stakeout box. Note how *layup* vehicles Alpha, Bravo, Charlie, and Delta are facing away from the target's vehicle, ready to pick up the follow and assume *command of the target* no matter which direction the target takes.

Equally important is the *trigger* vehicle. As shown in the illustration above, one of the ruses the FBI uses is to pull in and park ahead of the target's parked vehicle. This is called a *cheating* trigger. Being in front of the target, the FBI agent is less likely to attract suspicion, but he is still in a position to cue other members of the surveillance team when the target begins to drive away. This makes for a seamless transition from the *foot surveillance* team to the *vehicle surveillance* team.

In particular, the trigger vehicle transmits the start-time, direction of travel, and speed of the target's vehicle to the other members of the surveillance team. The appropriate layup vehicle can smoothly pick up the *follow* and assume command of the target because he has advance knowledge of the target's direction, etc., thanks to the radio transmission from the FBI agent in the trigger vehicle.

The lesson is obvious. Your adversary is the *entire* surveillance team, not just the FBI agents you happen to spot.

Exposing the FBI's secrets: Basic tactics...

Cover. Camouflage is an important component of an FBI vehicle surveillance operation.

FBI agents drive *anything and everything*, including sedans, coupes, utility vehicles, vans, trucks, four-wheel drive, minivans, commercial trucks, taxis, motorcycles, and even 18-wheelers.

Likewise, the FBI agents themselves come in all shapes and sizes. You'll see many different *silhouettes*. (That's spy-talk for the *personal appearance* of an agent.) When you're under FBI surveillance, you can expect to see singles, couples, families, seniors, disabled, rappers, and so on. Anybody with a pulse might be part of an FBI surveillance team.

A common mistake. If you're like most people, you might be thinking to yourself, *"There's no way they'd use a sweet little sixty-year-old grandmother."* Yeah, right. Grow up, and stop being such a patsy. The FBI loves *rubes* like you.

Or maybe you're thinking, *"No way they'd use a punk rapper with cranked-up music blaring from his car stereo."* Uh huh.

Start packing your toothbrush, doofus. Because the goons don't give you much time when they come a-knockin' an hour before dawn.

The most important lesson you'll ever learn. Any competent surveillance team – no matter which agency it's from – will use your preconceptions, prejudices, and personal biases *against you*.

So stop leaping to conclusions based on peoples' appearance.

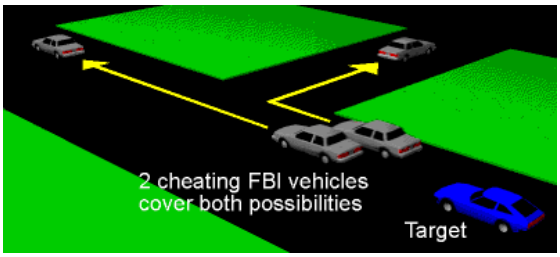
Go back and read that last sentence again. If you want to catch surveillance teams, you need to start evaluating people based on what they *do*, not what they *look like*. To catch spooks, you need to size people up by their *behavior*, not their *appearance*.

Fundamental tactics...

As you learned in the previous article in this series, the FBI utilizes a floating box to track you during a vehicle surveillance operation. The essential components of the box are the command vehicle, the backup vehicle, the left and right outrider vehicles, and the advance vehicle.

Under typical circumstances, the floating box is a powerful and versatile system of vehicle surveillance. The only occasions that cause concern to the FBI are when the target makes a turn. As you learned in the previous tutorial, a surveillance vehicle that follows a target around the corner is easy to spot.

The illustration below shows how the FBI has overcome this weakness.

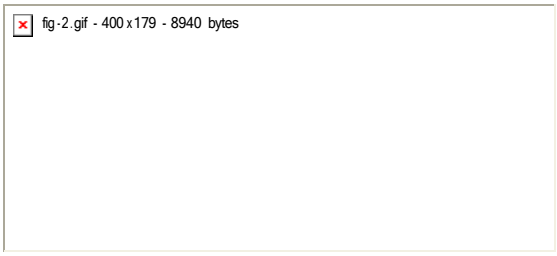


The cheating intersection. When the target is approaching a decision-point – and her direction of travel cannot be predicted by the FBI – the surveillance team leader makes certain that two FBI vehicles are in front of the target's vehicle. This is a deadly tactic. It has meant the ruin of many suspects who thought they could beat FBI surveillance.

NOTE – Disclosures about FBI tradecraft like this have never before been made public. This *Spy & CounterSpy* exclusive is possible only because our offices are just across the border in Canada, nine miles outside the reach of the FBI's goon squads.

As shown in the illustration above, each *cheating* FBI vehicle takes a different route. The FBI has every possible scenario covered. No matter which route you choose, a *cheating* FBI surveillance vehicle (positioned in front of you) has you covered.

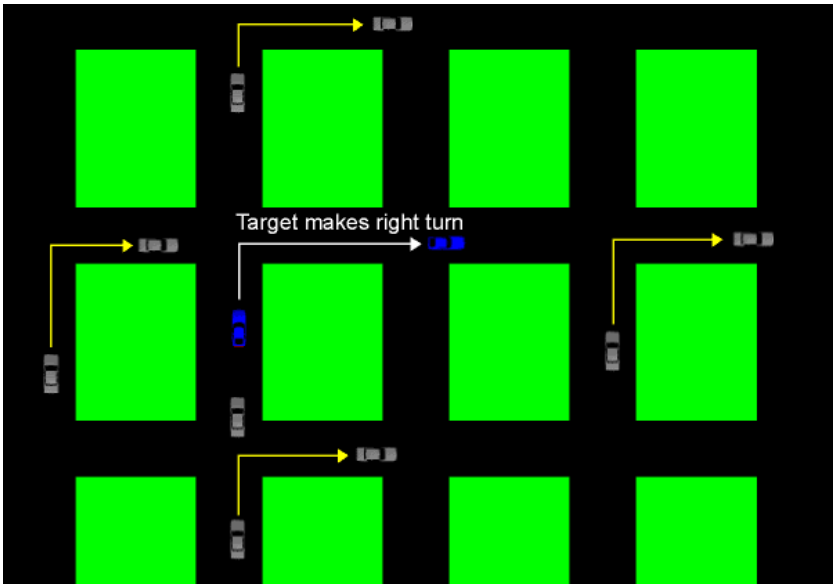
Many targets of surveillance have been repeatedly fooled by this tactic. The illustration below shows a more common implementation of this intersection maneuver.



At a typical intersection, the target vehicle can proceed in three different directions – left, right, or straight ahead. In a high-priority investigation where the FBI does not want to be detected, the team leader will place three surveillance vehicles ahead of the target. As shown above, each vehicle takes a possible route that the target might take. It doesn't matter which direction the target chooses, she is covered by a *cheating command vehicle*.

This technique is very difficult to detect in the short-term. (See the fourth tutorial in this five-part series for tips on how to provoke a surveillance team into revealing itself.) The technique is also expensive in terms of personnel and vehicles, so the FBI uses it mainly at major

intersections. Side-street situations are handled by the method depicted below.



How a floating box turns. When the target makes a right turn at an intersection, the right-side *outrider* also turns right – and becomes the new *advance* vehicle. As shown above, other members of the surveillance team also transform their roles.

The former *advance* vehicle becomes the new left-side *outrider*. The *backup* vehicle becomes the new right-side *outrider*. And the left-side *outrider* becomes the new *command* vehicle.

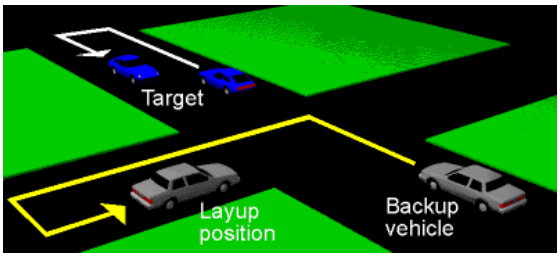
In the situation shown above, the former command vehicle usually continues straight through the intersection, so as not to attract attention to itself. It will be replaced by another FBI agent being held in reserve by the team leader.

The same principles apply when the target makes a left turn at a side-street intersection. Because this type of maneuver by the surveillance team results in predictable positions, an experienced target can use a deliberate turn as an *antisurveillance method* to detect the outriders and advance units of the surveillance team. For more information about antisurveillance and countersurveillance techniques, see the fourth tutorial in this five-part series.

Special situations...

An especially troublesome situation for the vehicle surveillance team is a sudden U-turn by the target. In many instances, the FBI has no way of knowing if the target simply missed his turn or if he is executing a deliberate antisurveillance or countersurveillance maneuver.

The illustration below depicts how the FBI typically responds to a sudden U-turn.



The backup vehicle immediately makes a left turn. This puts the FBI agent in a position to monitor the target and slip in behind him as he drives past. While this is happening, the other members of the surveillance team will be doing their best to redeploy in the new configuration.

Many newcomers who find themselves under FBI vehicle surveillance soon grasp the idea that U-turns are an effective way to befuddle the surveillance team. These *newbies* tend to make a U-turn and then try to detect vehicles "following" them. What they should be doing instead is watching for a vehicle making a quick left turn in

doing instead is watching for a vehicle making a quick left turn in response to the target's sudden U-turn.

ANTISURVEILLANCE TIP – Over a period of a few days, make a few unpredictable, sudden U-turns. If you see a pattern of vehicles turning away immediately after your U-turn, you may be under surveillance.

Diversions and decoys...

The FBI has become sophisticated in its use of diversions and decoys to cover the activities of its vehicle surveillance teams.

Diversion #1 – Tailgating. That inconsiderate driver tailgating you is not always just some *shmuck*. The FBI has found that this diversion is an excellent way to take your mind off other things that may be happening around you, like surveillance, for example.

Diversion #2 – Musical chairs. You're stopped at a red light, and the *bozo* in the car ahead of you gets out and rummages through his trunk. Yeah, right. You get the picture.

Diversion #3 – Confused drivers. They take forever to make a left turn. Or they straddle lanes. Or they start to make a turn, then change their mind and continue on. All of this happens directly in front of you, of course. It's an effective distraction. It's also an effective way to *delay you* while the rest of the surveillance team gets back into position after a mistake.

Diversion #4 – Sloppy drivers. This is the same maneuver as above, except that the FBI agent pretends to be a reckless driver. He might drive over the curb. He might speed and careen recklessly. Anything to get your mind off the situation and allow the other members of the surveillance team to escape detection.

Diversion #5 – Honey pots. The FBI will use pedestrians (attractive agents of the opposite gender) to distract you while you're driving. They use this ruse a lot more than most people realize. It's an incredibly effective way to divert the attention of the target. They'll also use customized cars and other eye-catching items or behavior to capture your attention.

Supporting the foot surveillance team...

FBI surveillance vehicles often contain one or two additional FBI agents *besides the driver*. This provides good cover. Most targets don't suspect a car containing a *group* of people.

This is not the reason, however, that the FBI uses groups. The extra people in the surveillance vehicle are there for a reason. They are important assets in the FBI's arsenal of surveillance tricks.

Foot surveillance. When the target parks his vehicle and sets off on foot, the vehicle surveillance team swtiches modes. The *wheel artists* immediately begin dropping off the *pavement artists* who will form a *floating box* around the walking target.

The vehicle surveillance team then assumes a *support role*, assisting the *foot surveillance* team. In particular, an FBI vehicle surveillance team will support the foot surveillance team in five ways.

Support Role #1 – Transition. The *wheel artists* drop off the foot agents in a *floating box* around a *target* who has just left his/her vehicle.

Support Role #2 – Leapfrogging. During the *foot follow*, the wheel artists will pick up, carry, and drop off FBI *pavement artists* at locations ahead of the walking target. This makes it easier to maintain a secure floating box around the target by leapfrogging members of the FBI team to locations where they are needed.

Support Role #3 – Communications. The vehicle surveillance team will provide reception and *rebroadcast* of the low-range body-communications equipment of the FBI *foot surveillance* agents. This is important in locations where radio reception can be difficult, such as high-density urban situations with concrete and steel buildings.

ANTISURVEILLANCE TIP – Look for a vehicle with a lone occupant at high elevation – atop a parkade, for example. During a foot surveillance operation in difficult terrain (downtown, for example), this FBI agent is positioned to receive weak transmissions from a *pavement artist* and rebroadcast them to the rest of the team.

Support Role #4 – Orientation. The *wheel artists* will provide *map* and *direction-finding* support to the pavement artists. This is particularly helpful during a *lost-command drill*, where the foot surveillance team has temporarily lost sight of the target. Map support also helps the foot surveillance team

anticipate upcoming obstacles.

Support Role #5 – Transportation. After the target returns to his/her vehicle, the vehicle surveillance team *picks up* the foot operators and *carries them* to the next location.

Conclusion. When implemented properly, the FBI's floating-box strategy is an effective vehicle surveillance system that gets results. Most targets never realize they're being watched. Those targets who manage to detect a *command* vehicle or *backup* vehicle are likely to be lulled into a false sense of safety by the *cheating* command vehicles and *cheating* intersection maneuvers. The mix of agent silhouettes and vehicles used by the surveillance team makes detection extremely difficult for the untrained target.

Coming up in Article #3...

In the next tutorial you'll learn about advanced methods of vehicle surveillance, like setups, traps, ambushes, and attacks. You'll also find out about psychological operations that the FBI can run against you while you're driving. You'll discover how they can use operant conditioning to covertly coerce you to alter your route – and leave you thinking it was *your* idea. Case studies supported by *custom-prepared* illustrations show you exactly how it's done.

Coming up in Article #4...

In the fourth tutorial you'll learn how to defend yourself against a vehicle surveillance team. You'll find out about *antisurveillance* – that's spy-talk for detecting the presence of vehicle surveillance.

You'll learn about the telltale patterns that give them away. You'll be able to detect them *without them realizing you've spotted them*. You'll see five maneuvers you can use while driving to trick them into revealing themselves.

You'll also learn about *countersurveillance* – that's spy-talk for obstructing and harassing a vehicle surveillance team. You'll see ten maneuvers you can use while driving to make things *very unpleasant* for the FBI.

Coming up in Article #5...

In the fifth tutorial you'll receive *step-by-step instructions* for breaking out of surveillance. You'll see how to give the goons the slip. You'll learn three methods for exploiting the flaws in the FBI's *floating-box* system.

The first method teaches you how to out-maneuver a *cheating command* vehicle and its backup unit. The second method shows you how to beat the FBI's *stakeout box*. The third method explains how to slip away while the goons are shifting from vehicle to foot surveillance.

In each case the FBI is forced to implement a *lost-command drill* in order to try and find you again.

How to make certain you get all the tutorials...

The next article is scheduled for publication in about two weeks. There are three ways you can ensure you don't miss any of the articles.

1. Visit our site regularly. *Spy & CounterSpy* is a living Web site, constantly growing, changing, evolving. We are involved in a continuing struggle to expose the tactics of the government's secret agencies. Return to our home page and bookmark our site. Visit us weekly – and you'll be assured of keeping up with the latest developments.

2. Become a member of *F9*. Return to our home page and click on *Free F9 membership*. In addition to receiving the free *F9* weekly bulletin, you'll receive email notification whenever a new article is posted at our Web site.

3. Get on our contact list. Simply click here to send email asking Vickie to add your name and your email address to our

asking Vickie to add your name and your email address to our contact list. We'll email you whenever we issue a news release or publish a new article at our Web site.

NOTE – If you're concerned about your personal privacy, please consider using a cyber-cafe and a *nom de guerre* with an anonymous free email account.

Spy school for the rest of us.

http://www.SPYCOUNTERSPY.com

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com
WEB SITE: http://www.SPYCOUNTERSPY.com

License and Limited Warranty

Spy & CounterSpy is an electronic magazine, hereinafter together with the information contained therein called the "product". By using the product you agree to the following terms and conditions. If you do not wish to be bound by these terms and conditions, do not use the product nor the information contained therein.

Spy & CounterSpy is published for information, education, entertainment and research purposes only. We are not security consultants – we are investigative journalists and survivors of surveillance. We are not rendering legal, accounting, management, security, tactical, political, or psychological counseling. If such advice is required the services of a competent professional should be obtained. We assume no responsibility for the accuracy of, or errors or omissions in, the information provided. In no event shall we be liable for any direct, indirect, consequential, special, or incidental damages arising out of the use of, or the inability to use, information described in the product. The names of persons, characters, corporations, institutions, organizations, geographic locations, products, and services used to explain and illustrate human behavior are entirely fictitious, except for the names of existing intelligence agencies, security services, and police agencies – or except as otherwise noted. No resemblance to actual individuals or entities is otherwise intended or implied.

License – *Here's-how, Right-now! Seminars Inc.* grants you, and you accept, a nonexclusive nontransferable license as follows for the product. You may use the product for your own use. You may make copies of the product on your hard disk and on floppy disk for backup purposes. You may print paper copies of the product for personal use. You may copy and distribute Internet-readable copies of the product by email, by link, by posting at your website, and for critical reviews and news reports in electronic or print form. You shall not otherwise modify or adapt the product using any means, electronic or mechanical, either in displayable form or as HTML source code. You shall not otherwise sell or transfer reproductions of the product to other parties in any way, nor rent, lease, or preview the product to other parties without the prior written permission of *Here's-how, Right-now! Seminars Inc.*

Limited Warranty – You expressly acknowledge and agree that use of the product is at your sole risk. The product is provided "as is" and without warranty of any kind, and *Here's-how, Right-now! Seminars Inc.* expressly disclaims all warranties, express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. No advertising, description, or representation, whether made by *Here's-how, Right-now! Seminars Inc.*'s agent, dealer, or employee shall be binding upon *Here's-how, Right-now! Seminars Inc.* or shall change the terms of this disclaimer or the limited warranty set forth herein. *Here's-how, Right-now! Seminars Inc.* does not warrant that the methods contained in the product will meet your requirements, or that the performance of the methods will be error-free, or that delivery of the product will be uninterrupted or error-free, or that defects in the product will be corrected. Furthermore, *Here's-how, Right-now! Seminars Inc.* does not warrant or make any representations regarding the use or the results of the use of the product in terms of its correctness, accuracy, reliability, or otherwise. No oral or written information or advice given by *Here's-how, Right-now! Seminars Inc.* or its authorized representatives shall create a warranty or in any way increase the scope of this limited warranty. Should the product prove defective, you (and not *Here's-how, Right-now! Seminars Inc.*) assume the entire cost of all necessary correction, repair, treatment, or servicing. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. *Here's-how, Right-now! Seminars Inc.* shall not be liable for special, incidental, consequential, or other damages, even if *Here's-how, Right-now! Seminars Inc.* is advised of or aware of the possibility of such damages. This means that *Here's-how, Right-now! Seminars Inc.* shall not be responsible or liable for lost profits or revenues, or for personal injury, or for damages or costs incurred as a result of loss of time, data, or use of the product, or from any other cause. In no event shall *Here's-how, Right-now! Seminars Inc.*'s liability exceed the purchase price, if any, of the product. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. The author and publisher of the product have used their best efforts in preparing the product and the material contained in it. These efforts include the research, development, and testing of the theories and methods in order to determine their effectiveness. The author and publisher make no warranty of any kind, express or implied, with regard to the techniques contained in the product. The author and publisher shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of the techniques, associated instructions, and/or claims of productivity gains.

SPY & COUNTERSPY

Providing knowledge and skills to supporters of freedom and fairness.

Spy & CounterSpy Exclusive Report

Uncrackable Email

Part 1 in a two-part series

Assumption – You are a typical American.
Question – Is the FBI reading your encrypted email?
Answer – Probably not.
Now the same question, but this time a different assumption.
You are an American under surveillance by the FBI.
Question – Are they reading your encrypted email?
Answer – Yes. Absolutely.

How surveillance is triggered...

Dissidents pose no danger to the country. It is the conformist who poses the greatest danger to our freedoms.

If you are involved in anything like advocacy, dissent, or protest, then you are inviting surveillance. Anything that challenges the status quo – *no matter how mild* – is viewed with suspicion by the authorities. Sometimes the simple act of expressing an honest opinion or writing a letter to the editor is all it takes for a security service like the FBI or BATF to start nosing around. Independent thought is becoming a rare – and dangerous – attribute in America. Bureaucrats don't understand that dissent poses no danger to the country. On the contrary, it is *the conformist* who poses the greatest danger to freedom.

There are thousands of regulations, prohibitions, rules, restrictions, laws, bylaws, codes, and statutes designed to regulate your behavior. It's common knowledge that any cop worth the badge can find *something* to arrest you for. More than ever, ordinary Americans are finding it necessary to shield their activities from a government whose red tape can prevent you from earning a living, developing your land, etc. etc. etc.

The Thought-Police. Once you're under surveillance, the simple act of encrypting your email is all it takes for the FBI to label you dangerous, perhaps a threat to national security.

Like many repressive regimes worldwide, the US government doesn't understand that people who want privacy *aren't necessarily hiding anything*. You put letters inside envelopes, don't you? Well then, doesn't it make sense to encrypt your email? Otherwise it's like sending a postcard. Anybody can read it along the way.

PGP is under attack. PGP is considered the best encryption software available for use with email. But despite its robustness, PGP is regularly beaten by the FBI. Surveillance teams routinely read PGP-encrypted email.

That's because most people aren't using PGP correctly. If you are one of them, you are vulnerable. The FBI possesses the means to mount a sophisticated covert campaign against you. They can choose from an arsenal of proven methods for cracking your PGP-encrypted email. Those methods are described in this document.

Assessing the threat. When the FBI succeeds at decrypting your messages, it is unlikely you will realize that you have been compromised. But having your email decrypted and read is not the prime threat. You face an even greater danger from an FBI surveillance team – *especially if you are a member of a group that is targeted by the FBI*.

The FBI has decades of experience. They have learned to wring every possible advantage from each situation. They play by *Big Boys' Rules*. The FBI's goal is not only to get you, their goal is to wreck your entire group.

How do they manage to do this? By deception. Once they've

cracked your PGP email, they will begin to create *forged messages*. They will impersonate you. The FBI team will send bogus email messages that seem to come from you. They will systematically work to create confusion, suspicion, and paranoia throughout your group.

This is the real nature of the threat. If the FBI cracks your communication they won't stop at getting you. They want the whole group – or organization, team, cell, family, squad, or whatever it's called.

How they do it. In this tutorial you're going to learn about the different methods that the FBI uses to crack your PGP system. Some of these attacks may come as a surprise to you. Many of these attacks are also used by other agencies like the BATF, DEA, CIA, and even local police.

What you can do about it. This tutorial will show you different ways you can use PGP. These protocols reduce – and occasionally eliminate – the ability of the goons to crack your messages. And as a bonus, you're going to learn how you can use your email to conduct aggressive *antisurveillance* against the FBI – perhaps exposing a surveillance team that you didn't realize was watching you..

How the FBI cracks PGP email...

The FBI has resources and expertise. Their methods fall into four categories. Method 1 relies on their ability to break into your home or office undetected. Method 2 relies on their ability to bug your home or office. Method 3 uses electronic equipment that detects signals your computer makes. Method 4 is used in cases involving national security, where they rely upon the cryptanalysis capabilities of NSA.

SPY & COUNTERSPY

Know where you're vulnerable. The weakest part of your email security is you, the user. The mathematical algorithms that form the underpinnings of PGP are very robust. It is the manner in which you use them that creates vulnerabilities.

The most vulnerable point is the manner in which you create and store your original plaintext message. The next weakest element is your passphrase. Next are the PGP files on your computer's hard disk. (From now on we'll refer to your hard disk drive as HDD).

In a typical surveillance operation, the FBI will utilize the attacks described here. The ten attacks are listed in approximate order of increasing difficulty. It is standard operating procedure for the FBI surveillance team to use the simplest attacks first. In practice, their choice depends on the circumstances of the case.

Attack #1 – Plaintext recovery. An FBI or BATF surveillance team will break into your home or office *without your knowledge*. Once inside, the agents will read the plaintext files on your hard disk, diskettes, or paper printouts. Local police also use this method. It is very effective.

If you're like most people, you're probably thinking to yourself, *"Aww, there's no way they could get in here without me knowing. I'd spot it right away."*

Yeah, right. That's exactly the attitude the FBI wants you to have. So dummy up. FBI penetration agents love people like you. You are the ideal target. Over confident. Easy to deceive.

This is important enough for us to pause for a few moments and talk a bit about how surveillance teams really operate. What you are about to read has *never been published before*. The government does not want you to know this.

Background – How they get inside. Many people are amazed to learn their home or office can be entered without their knowledge. And not just once, but *repeatedly*. A surveillance team often requires multiple entries in order to thoroughly pick through all your stuff.

Good quality locks on your doors and windows are generally useless. The penetration team ignores them. They've found *an easier way to get inside*. Perhaps an example is the best way to illustrate the point.

Case Study. Ever since we launched *Spy & CounterSpy*, we have been involved in running battles with FBI surveillance teams trying to get inside our offices. Because of our experience we are not an easy target. Their operations were complicated by the fact that the

Top: Dislodged block, exterior wall.
Below: Cabinet against exterior wall.

FBI is *operating illegally* in Canada and must act covertly at all times.

The setup. Our former office was situated in an industrial park. We were located in a cindercrete masonry building equipped with high-security locks. We concluded it would be difficult for an FBI surveillance team to conduct a surreptitious entry without our knowledge.

Our building abutted a similar cindercrete building next door – a welding shop. The bathroom cabinet sink is located against this wall. The arrangement provided *a perfect opportunity for surreptitious entry*.

The photos tell the story. It's easy for FBI agents to enter a building next door and remove a few cindercrete blocks from two sets of exterior walls – and then enter our office through the back of the bathroom cabinet.

Repair experts. Most people aren't aware that surveillance teams routinely break in through walls, ceilings, and up through floors. This is *standard operating procedure*. The FBI's restoration specialists can repair a damaged area in under *90 minutes* using patch drywall, quick-drying compound, and special paint. Apartments and houses are a snap for these guys. This is your own government doing this to you, folks.

My first experience with this sort of entry was when I was helping Vickie deal with 24-hour surveillance by US Naval Intelligence. (Return to our home page and click on *About Us* for more on this.) I showed her how to seal her house – doors, windows, attic panel, everything.

But they tunneled over from the house next door. They came in under the driveway and broke through behind a false wall next to a fireplace in the downstairs family-room. They moved along a short crawlspace and entered the livingspace just behind the furnace.

Their cover was clever. They used a ruse of major renovations next door to conceal the sound the tunnel crew made.

Their mistake? Not enough attention to detail. They didn't match the original panel when they replaced the wall behind the furnace. Vickie and I had done a complete inspection of her house two months earlier. We both spotted the bogus panel immediately. She still becomes*furious* when she talks about it.

The reason the goons like to break in through walls is simple – it's extremely difficult to defend against. But simply being able to detect that you've been penetrated gives you an advantage, especially if you don't reveal you're on to them.

Now that you've got a better understanding of how resourceful and cunning these *government agents* are, let's return to the different attacks they use to crack your encrypted email. We've already covered Attack #1, plaintext recovery.

Attack #2 – Counterfeit PGP program. After breaking into your home or office, FBI agents will install a *counterfeit copy* of PGP on your HDD. Encrypted messages created by this modified program can be decrypted with the FBI's *master key*. It can still be decrypted by the recipient's key, too, of course.

Their goal is to grab your secret key and your passphrase so they can use any copy of PGP to read your email.

A variation of this attack is the FBI's *bot*. Acting similar to a virus, the bot is a *key-trap program*. (Bot is an abbreviation of robot.) The bot intercepts your keystrokes without your knowledge. When the opportunity arises, the bot uses your *Internet dial-up connection* to transmit your passphrase to the surveillance team. FBI agents often hide bots in counterfeit copies of your word processing program, and so on.

Attack #3 - PGP's working files. After entering your premises in your absence, FBI agents will make copies of certain PGP files on your HDD, especially the files containing your secret keys. The agents will then attempt to find where you've written down your passphrase. They'll methodically search your papers, desk, safe, filing cabinets, kitchen drawers, and so on. They'll use deception to gain access to your wallet, purse, money belt, briefcase, and pockets.

Their goal is to grab your secret key and your passphrase so they can use *any copy* of PGP to read your encrypted email messages whenever they want.

If their search fails to turn up your passphrase, they'll use *cracker software* to deduce it. This works because most people use passwords and passphrases consisting of words and numbers with special meaning like birth dates or pet names. Unfortunately, it's a

special meaning like birth dates or pet names. Unfortunately, it's a simple matter for the FBI to collect information about you like your birth date, your mother's maiden name, the number of a PO Box you rented 10 years previous, the license plate of your vehicle, names of pets past and present, and so on.

Here's how the FBI's cracker software works – it combines and recombines all these words and numbers and keeps submitting them to the PGP program. (They copy *your entire HDD* and do this work at their office.) They routinely crack the passphrases of PGP-users who fail to use random characters in their passphrase.

Attack #4 – Video surveillance. After breaking into your home or office without your knowledge, FBI specialists will install a miniature video surveillance camera above your work area. The lens is the size of a pinhead. It's extremely difficult to detect. The FBI surveillance team watches your fingers on the keyboard as you type in your passphrase. Local police and private investigators have also been known to use this method.

Attack #5 – Audio surveillance. This method is a variation of Attack #4. FBI technicians install an audio bug near your computer. The sounds generated by the keyboard can be analyzed. By comparing these sounds with the noises made during generation of a *known piece of text*, the FBI can often deduce your passphrase – or come so close that only a few characters need to be guessed.

Attack #6 – AC power analysis. Using equipment attached to your *outside power lines*, the FBI can detect subtle changes in the current as you type on your computer's keyboard. Depending on the user profile in your neighborhood, the FBI's equipment can be located some distance from you.

Attack #7 – EMT analysis. EMT is an acronym for electromagnetic transmission. Computer CPUs and CRTs operate somewhat like radio transmitters. CPU is an acronym for central processing unit. This is your Pentium chip. CRT is an acronym for cathode ray tube. This is your display.

The FBI surveillance team uses a communications van (or motor home) parked across the street to capture the electromagnetic transmissions from your computer. This threat can be eliminated by a shielding system called *Tempest*. In many jurisdictions you need a special permit to buy a Tempest system, however.

Attack #8 – Coercion. The previous seven attacks are quite easy for the FBI to implement. In fact, they use almost all of them on a routine basis. Even the local police in major US cities have access to vans that can pick up your computer's EMT.

From this point on, however, things start to get very time-consuming and expensive for the FBI in their attempt to crack your PGP-encrypted email. So they may decide to take a more direct approach.

They'll simply bend your thumb back. *Until it breaks, if that's what it takes*. Before they start, they'll make sure they've got enough *biographical leverage* on you to blackmail you into becoming an informant. Biographical leverage is spy-talk for blackmail information.

The main defense against this threat is deception. An appropriate strategy is discussed later in this tutorial.

Attack #9 – Random numbers. After breaking into your home or office without your knowledge, FBI agents will make a copy of PGP's *randseed.bin* file. PGP uses the pseudorandom data in this file to help it generate a unique block that it uses for creating a portion of the ciphertext. This type of attack borders on true *cryptanalysis*. It is time-consuming. It is expensive. It is generally worth neither the FBI's nor NSA's time, except in cases of national security.

Attack #10 – Cryptanalysis. It is ridiculously easy for anyone, including the FBI, to intercept email on the Internet. After collecting a sampling of your encrypted email, the FBI submits the data to NSA for cryptanalysis. Cryptanalysis is egghead-talk for using mathematics, logic, and problem-solving skills to crack an encrypted message. It's all done with computers – and NSA has some *monster* computers.

The best information available to us indicates that NSA can indeed crack PGP email, but a *brute force attack* is required. A brute force attack involves a lot of informed guessing. It's mostly just trial-and-error. Cracking a message can take weeks, months, years, or decades depending on the content, format, and length of your message. Later in this tutorial you'll see how to make your messages more resistant to this attack.

Very few domestic cases warrant the involvement of NSA. Besides, FBI agents are usually successful in cracking your email

Besides, FBI agents are usually successful in cracking your email using one of the other attacks, especially *break-and-enter*. So NSA devotes its resources to cracking the messages of other countries' governments and their intelligence agencies.

Thinking outside the box...

The preceding ten attack-scenarios are based on thinking inside the box. When we use this type of reasoning, we are staying within a set of fixed assumptions. We are, in effect, boxed in by our rigid assumptions – hence the phrase, thinking inside the box.

The preceding attack-scenarios make two assumptions. First assumption – You've got an authentic copy of PGP. Second assumption – NSA has not yet discovered a mathematical method for decrypting PGP ciphertext. Neither assumption is necessarily correct.

Counterfeit software. We have received one report about this. We must caution you that it is only one report, and we have been unable to verify it through other sources. Our contact says an FBI agent bragged to him that the CIA has been distributing doctored copies of PGP freeware over the Internet. According to our source, the FBI routinely decrypts messages encrypted with these doctored copies.

It is our view that if this happened it was not over a wide-scale. Many copies of PGP are digitally signed by the manufacturer, who is no dummy. We believe that the fragmentary and decentralized character of the Internet prevents this type of ruse from succeeding – especially against savvy targets like the folks at PGP.

Mathematical algorithm. It is unlikely that NSA has developed a mathematical algorithm for decrypting PGP ciphertext – not impossible, but unlikely. Because the algorithm and the source code for PGP are widely known and freely available, PGP has been subjected to rigorous testing and attacks by some of the brightest minds in the scientific community. This is called a *review by your peers*. It is a powerful method for vetting new ideas and methods. None of these bright scientific minds have come close to cracking the PGP algorithm, which is based on a complicated *one-way math function*.

Sizing up your adversary...

Clearly, FBI and BATF surveillance teams are a force to be reckoned with. They possess a lethal arsenal of capabilities that they can bring to bear against you and your email privacy. Their methods range from the simple to the sublime. They can break into your home or office without your knowledge and use your computer. They can use sophisticated electronic equipment to read your keystrokes – over the AC electrical connection, over the telephone line, or over the airwaves. And, finally, if these types of methods fail – which isn't very often – NSA will be called in to crack your PGP-encrypted message.

Is the FBI difficult to beat? Yes. They've been at this game a long time. They've learned many lessons over the years.

Can the FBI be beaten? *Yes, you can beat them.* It is easy? No, not at first, but it gets easier as you build up self-discipline. Beating the FBI requires that you stop thinking inside the box.

Part 2 of this tutorial will show you how.

To stop the FBI from reading your PGP-encrypted email, return to our home page now and click on *Uncrackable Email 2*.

Back to Home Page

such advice is required the services of a competent professional should be obtained. We assume no responsibility for the accuracy of, or errors or omissions in, the information provided. In no event shall we be liable for any direct, indirect, consequential, special, or incidental damages arising out of the use of, or the inability to use, information described in the magazine. We are not responsible for typographical errors, browser performance, or email client idiosyncracies. The names of characters, corporations, institutions, organizations, products, and services used to illustrate human behavior in this publication are entirely fictitious, except for the names of existing intelligence agencies, security services, and police agencies. No resemblance to actual individuals or entities is otherwise intended or implied.

LICENSE -- *Here's-how, Right-now! Seminars Inc.* grants you, and you accept, a nonexclusive nontransferable license as follows for *Spy & CounterSpy*, an electronic magazine hereinafter called the "product". You may use the product for your own use. You may make copies of the product on your hard disk and on floppy disk for backup purposes. You may print paper copies of the product for personal use. You may copy and distribute Internet-readable copies of the product by email, by link, by posting at your website, and for critical reviews and news reports in electronic or print form. You shall not otherwise modify or adapt the product using any means, electronic or mechanical, either in displayable form or as HTML source code. You shall not otherwise sell or transfer reproductions of the product to other parties in any way, nor rent, lease, or preview the product to other parties without the prior written permission of *Here's-how, Right-now! Seminars Inc.*

Limited Warranty

You expressly acknowledge and agree that use of the product is at your sole risk. The product and related documentation are provided as is and without warranty of any kind, and *Here's-how, Right-now! Seminars Inc.* expressly disclaims all warranties, express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. No advertising, description, or representation, whether made by *Here's-how, Right-now! Seminars Inc.*'s agent, dealer, or employee shall be binding upon *Here's-how, Right-now! Seminars Inc.* or shall change the terms of this disclaimer or the limited warranty set forth herein. *Here's-how, Right-now! Seminars Inc.* does not warrant that the methods contained in the product will meet your requirements, or that the performance of the methods will be error-free, or that delivery of the product will be uninterrupted or error-free, or that defects in the product will be corrected. Furthermore, *Here's-how, Right-now! Seminars Inc.* does not warrant or make any representations regarding the use or the results of the use of the product or related documentation in terms of their correctness, accuracy, reliability, or otherwise. No oral or written information or advice given by *Here's-how, Right-now! Seminars Inc.* or its authorized representatives shall create a warranty or in any way increase the scope of this limited warranty. Should the product prove defective, you (and not *Here's-how, Right-now! Seminars Inc.*) assume the entire cost of all necessary correction, repair, or servicing. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. *Here's-how, Right-now! Seminars Inc.* shall not be liable for special, incidental, consequential, or other damages, even if *Here's-how, Right-now! Seminars Inc.* is advised of or aware of the possibility of such damages. This means that *Here's-how, Right-now! Seminars Inc.* shall not be responsible or liable for lost profits or revenues, or for damages or costs incurred as a result of loss of time, data, or use of the product, or from any other cause. In no event shall *Here's-how, Right-now! Seminars Inc.*'s liability exceed the purchase price of the product. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. The author and publisher of the product have used their best efforts in preparing the product and the material contained in it. These efforts include the development, research, and testing of the theories and methods in order to determine their effectiveness. The author and publisher make no warranty of any kind, express or implied, with regard to these techniques or the documentation contained in this product. The author and publisher shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of the techniques, associated instructions, and/or claims of productivity gains.

SPY & COUNTERSPY

Providing knowledge and skills to supporters of freedom and fairness.

Spy & CounterSpy Exclusive Report

Uncrackable Email

Part 2 in a two-part series

In Part 1 of this two-part tutorial, you learned about the methods that FBI surveillance teams use to crack your PGP-encrypted email messages. Many of those methods involved breaking into your home or office *without your knowledge*. Some methods involved electronic devices in a communications van located a short distance from your home or office – across the street perhaps. (If you haven't read Part 1, you might want to go back and do so now before reading further. Return to our home page and click on *Uncrackable Email 1*.)

Uncrackable Email Part 2 describes ways to protect your email privacy – and the secrecy of your messages. These methods work against the FBI, BATF, DEA, and other government agencies, including state and local police.

You'll learn step-by-step protocols and countermeasures that you can implement. In some cases, these methods will stop an FBI investigation *cold*. In other cases, they will only delay it. Much depends on the circumstances of the case. *A lot* depends on your countersurveillance and antisurveillance skills.

Each solution described in this tutorial is a *protocol*. You can think of a protocol as a method, a set of guidelines, or an operating procedure.

Flexibility. If your goal is to absolutely prevent the FBI from cracking your PGP-encrypted email, the key to success is flexibility. The content of your email is what counts. The more incriminating the message, the more precautions you should take.

Protocol 1:
The firewall method...

When used properly, the firewall method can completely frustrate an FBI surveillance team.

The firewall method is centered on the way you use your computer. This includes where, when, and how you use your computer. Described here is a step-by-step method for obstructing the FBI. This is a very rigorous protocol. You likely won't need to go to this much trouble very often.

Step 1 – Get cleaned up. Scrub your hard disk. The FBI can read deleted files using an *undelete utility*. The FBI can read file slack, RAM slack written to disk, free space, garbage areas, and the Windows swap file using a *sector viewer* or *hex editor*. Return to our main page and click on *Security Software* for more on this. Although other packages are available, we use Shredder™. Then we use Expert Witness™ and HEdit™ to check the hard disk afterwards. (From now on we'll refer to your hard disk drive as HDD.)

If you have previously used your computer to work with incriminating data, you should wipe the *entire* HDD and reinstall the operating system, application software, and user files. If surveillance poses a risk to your liberty, you must install a new hard disk drive. Then disassemble the old HDD, remove the platters, and sand them with coarse-grit sandpaper.

Once you've got your computer sterilized, you'll want to keep it clean. Tidy up after each work session. Thereafter, don't leave your computer unattended.

Step 2 – Get unplugged. During sessions when you're working on secret messages, you should take measures to frustrate FBI

surveillance. This means *physically disconnecting* your computer from the AC power supply and from the telephone jack. You'll need a battery-powered computer – a laptop, notebook, or subnotebook.

Remaining connected to the AC power supply is risky. Using equipment attached to your power line outside your home or office, the FBI can detect subtle changes in the current as you type on your computer's keyboard.

Likewise, remaining connected to the telephone line is risky. If the FBI has broken in without your knowledge, they may have installed *counterfeit programs* on your computer. Your computer could be secretly sending data to the surveillance team over your *dial-up connection*. Just imagine the damage if you were unknowingly using a *doctored copy* of your favorite word processing program.

Step 3 – Go somewhere else. In order to frustrate the FBI's electronic surveillance capabilities, you must relocate away from your usual working area. If you fail to take this step, an FBI video camera can watch your keystrokes. An FBI audio bug can listen to your keystrokes. An FBI communications van parked in the neighborhood can detect both your keystrokes and your display.

Suitable locations for ensuring a surveillance-free environment are park benches, crowded coffee shops, busy fast food outlets, on a hiking trail, at a friend's place, in a borrowed office, at a bus depot waiting area, in an airport lounge, at the beach, and so on. Be creative and unpredictable. The trick is to select a location difficult for FBI agents to watch *without you becoming aware*.

You may be surprised at what happens the first time you relocate. If you suddenly find people loitering nearby, you may *already* be under surveillance. (More about this later in the tutorial.)

During your first relocated work session, use PGP to create your secret key ring. Your passphrase should contain random characters. Do not write down your passphrase. If you must, jot down just enough hints to help you remember.

Save copies of the following files from the PGP directory to a diskette – *Secring.skr, Secring.bak, Pubring.pkr, Pubring.bak*, and *randseed.bin*. For safety, use two diskettes and make two backups. Keep the diskettes on your person. Delete the files from your HDD.

Step 4 – Get serious. From now on, you've got a *new* standard operating procedure. Whenever you need to compose and encrypt a secret message, you must first relocate to a safe area. (You'll soon begin to appear like a busy person who checks in often with your contact software or scheduling software.)

Save the encrypted document to diskette. Delete all working files. Return to your home or office. Then use *a different computer* to email the encrypted messages.

Using a different computer is *vital*. It acts like a firewall. It keeps your relocatable computer sterile. Do not connect your relocatable computer to the telephone line. *Ever*. Do not leave your relocatable computer unattended. *Ever*. If this means carrying your relocatable computer with you all the time, then so be it.

For ordinary working sessions, it's usually okay to connect your relocatable computer to AC power. However, don't do any sensitive work in this mode. Always disconnect and relocate first. But if *absolutely watertight security* is your goal, the only time you'll turn on your relocatable computer is when you've relocated. The only time you'll plug it in is to *recharge the battery*.

When you receive incoming encrypted email on your firewall computer, save it as a text file to diskette. Relocate. Check the diskette with an antivirus program. Load the file into your sterile computer. Decrypt the ciphertext and read the plaintext. Delete the plaintext. Return to your regular work location.

Summary. The firewall method involves *nit-picking attention to detail*. It is a methodical system for protecting the privacy of your PGP-encrypted email messages. It takes perseverance and patience to beat the FBI at this game. But it's preferable to the alternative. The firewall method will keep you out of the *internment camps*.

You'll read about other protocols later in this tutorial. But if you choose to use the firewall method, you must follow it rigorously in order for it to be effective. Slip up once and the goons *will* nail you. They'll snatch your passphrase. They'll learn where you keep your key rings. Then it's interrogation, arrest, indictment, conviction. *Or maybe they'll just kick in the door an hour before dawn and ship you off to the camps.*

The firewall method is watertight, but it only works if you use it.

The firewall method is watertight, but it only works if you use it.

Protocol 2:
The deception method...

SPY & COUNTERSPY

Protocol 2 is based on liveware, not software. Liveware refers to *you*, the human element in the countersurveillance scheme. Protocol 2 takes a human approach. It uses deception.

Most people don't realize that *FBI surveillance teams are vulnerable to deception*. It's possible to mislead and confuse them. That's because most FBI targets are ordinary Americans with no countersurveillance training. In relative terms, *only a few elite units* within the FBI encounter hard targets. (A hard target is a trained operative who is actively maintaining secrecy and who will not reveal that he has detected the surveillance team.) So most FBI agents *have never confronted a hard target*. They never get any practice. They're accustomed to playing tennis with the net down.

Deception provides four ways for you to protect the privacy of your PGP email.

Deception method 1 – Decoy. This method involves duping the surveillance team into believing they have cracked your PGP email, when in fact they have uncovered merely a decoy. Your real protocol continues to run *undetected* in the background. This is called layered security.

The best underground activists worldwide operate in this manner, including guerrilla movements, freedom fighters, and resistance groups. Inside the USA this method is mostly used by criminal groups (so far).

The key to success is carefully and deliberately providing some *mildly incriminating evidence* for the FBI to find. This decoy data will often dissuade them from investigating further. The FBI will eventually downgrade the 24-hour surveillance to perimeter surveillance, then picket surveillance, and finally intermittent surveillance. They'll keep you on their *watch-list* and check up on you two or three times a year. They may drop you entirely. Here's how to implement this method.

Step 1 – Set up *Protocol 1* and then forget about it.

Step 2 – Use your *firewall computer* as your primary computer. Create another set of secret keys. Leave the key ring files and *randseed.bin* on your HDD. This increases the chances the FBI will recover them during a surreptitious entry. Create and encrypt low-grade messages at your firewall computer. This increases the odds that the FBI will snatch your passphrase.

Step 3 – Use this second configuration of PGP as a decoy. Use it to send only *low-grade messages*. In effect, you are now running two layers of PGP. From time to time you will use *Protocol 1* and temporarily relocate in order to encrypt or decrypt *high-risk secret messages*.

Step 4 – If you suspect or detect FBI surveillance, keep up the deception. Perhaps temporarily stop using your relocatable computer. If you use the technique of *plausible denial*, you increase your chances of completely concealing the fact that you've got a second PGP system.

The principle of plausible denial is well-known in intelligence agencies, urban guerrilla movements, and resistance groups. Plausible denial means *cover*. Cover is spy-talk for innocent explanation. You must take the precaution of having a plausible, innocent explanation for everything you do. *Absolutely everything*. Don't ever do anything until you think up a believable excuse for doing it.

Even if the FBI surveillance team discovers the second protocol, you will have purchased yourself some extra time. Use the time to encrypt, conceal, or destroy incriminating data. Use the time to warn other members in your group. Use the time to *feed misinformation* to the surveillance team.

When systematically applied, the decoy method provides a good first line of defense against an FBI surveillance team.

Deception method 2 – Thwarting cryptanalysis. When using Protocol 1, you can utilize deceptive techniques to reduce the chances of your message being cracked by NSA. If the case is serious enough, the FBI will provide NSA with a full set of your encrypted messages.

The cryptanalysis experts at NSA will use *Statistical Probability Analysis* to begin detecting commonly used phrases, words,

punctuation, and layout. The more footholds you give them, the sooner they'll crack your email. Here are three ways to use deception to impede their progress.

Step 1 – Disguise the *format* of your message. Your goal is to camouflage the layout. Insert a random-length paragraph of *nonsense* at the beginning of each message. You do not want the salutation or other material to appear at always the same location. Your recipients should be alerted to ignore the first paragraph. You can also use a text editor to manually *strip off* the header and footer from PGP ciphertext. The recipient can likewise use a text editor to manually restore the header and footer so PGP will recognize the text as code to be decrypted.

Step 2 – Make your content *resistant to heuristic analysis*. Heuristic analysis involves informed guessing and trial-and-error. Deliberately run some words together, eliminating the space. Intentionally add or delete punctuation. Occasionally insert a carriage return in the middle of a paragraph. Deliberately introduce spelling errors into your text.

Step 3 – Write your message in a "foreign" language. You can do this by using *homonyms* such as "wood" instead of "would", or "urn" instead of "earn". Use "gnu" or "knew" instead of "new". Use "seas" instead of "seize". Use "mast" instead of "massed". Write numbers and dates out in full, such as "nineteen ninety eight" instead of 1998. Use code words such as *competition* instead of surveillance, *competitor* instead of FBI, *market survey* instead of countersurveillance, and so on. Use *noms de guerre* instead of real names.

When properly used, these and other anti-cryptanalysis techniques can greatly increase the amount of time it takes the NSA to crack your PGP-encrypted email.

Deception method #3 – Diagnostics. You can use PGP to *detect the presence* of a surveillance team. Countersurveillance experts refer to this as running *diagnostics*. When performed against pavement artists, it is called *dry-cleaning*. Here's how it works.

Deliberately encrypt a provocative, bogus series of messages. Your goal is to use content that will elicit *an aggressive response* from the FBI. If surveillance intensifies, your email may have been cracked – or the FBI may simply be reacting to your *increased traffic*. That's spy-talk for the frequency, volume, and timing of your messages.

On the other hand, you may notice that the surveillance team seems to know where you're going and who you're going to meet with. They arrive *before you do*. They break into your associate's home or office looking for items *you've mentioned in your email*. They're conspicuously nearby as you slip a written note to your contact, after mentioning the brushpass in your email.

All these are *warning signs* that the FBI is reading your PGP-encrypted email. If you're using a decoy setup, switch to Protocol 1 to send secure email. If you're already using Protocol 1, you and your correspondents should create *new passphrases*. If further diagnostics suggest the FBI is still reading your email, you and your correspondents should reinstall PGP and create *a fresh set of key rings and passphrases*. Exchange the key rings by face-to-face contact, through live intermediaries, or by human courier.

Tip – Anonymous email addresses activated through a cyber caf□□an be used, but only if you set them up before the FBI puts you under surveillance. Go out and do it tomorrow.

When properly applied, diagnostics can keep you *one step ahead* of an aggressive FBI surveillance team.

Deception method #4 – Spoofing. You should routinely send out *bogus* encrypted messages. Your goal is to mislead and confuse the surveillance team. If the FBI is reading your email, you have an opportunity to confuse and mislead them with *misinformation*. If the FBI hasn't cracked your email yet, the traffic in bogus messages will provide *cover* for your *authentic messages*. If a mission requires an increased number of secret messages, simultaneously reduce your bogus messages, and the FBI won't detect any increased communication activity.

When used systematically, spoofing can level the playing field between you and the FBI surveillance team.

Summary...

You can boost your chances of stopping an FBI surveillance team

Using deception, you can confuse, mislead, obstruct, and frustrate the surveillance activities of your adversary. Deception can be *very effective* against an FBI, BATF, or DEA surveillance unit. It is

from learning anything at all.

particularly effective against standard police surveillance.

If the deception techniques of *Protocol 2* are used in combination with the firewall methods of *Protocol 1*, you boost your chances of stopping an FBI surveillance team from learning anything at all.

Back to Home Page

License

Limited Warranty

SPY & COUNTERSPY

Providing knowledge and skills to supporters of freedom and fairness.

Situation Report

Bureaucrat's Toolkit

Secret methods of political control over the American people...

You're about to lose something. It's already slipping from your grasp. And once it's gone, you'll never get it back.

As a people, we are facing the most serious threat to humanity in recorded history – the systematic stripping away of traditional freedoms by governments worldwide. And that includes *all* governments.

It is a situation far more serious than the plagues of the Middle Ages that nearly wiped us out as a species. It is a threat never before seen in ten thousand years of human history.

You are about to become the property of the government.

A question of control...

Governments today have the means to permanently wrest control from their populations.

A number of separate threats have recently converged. An extremely dangerous situation has been created. Governments have been given the opportunity – and the means – to *permanently* wrest control from their populations. Bureaucrats are about to realize their dream of *absolute power*. It is a nightmare far worse than anything George Orwell might have imagined.

Technology is providing the tools to government. We are now at a point in human evolution where your government – if it so chooses – can control every aspect of your life *from cradle to grave*.

We face three separate threats. Together these threats combine to give government a stranglehold on our civil liberties – a death grip on our traditional freedoms.

Threat #1 – Computers have taken over surveillance. Surveillance is now automated. Entire populations can be supervised and monitored in real time. Half your life, including your last credit card purchase, is already on a database. Computers eavesdrop on all electronic and telephone communications using word-recognition and voice-recognition software. Video cameras are everywhere – inside and outside – they can recognize vehicle license plates and even human faces. And all this information, all these databases, are cross-referenced and tied together – by computers. Taken together, it's called *dataveillance*. It makes it easy to track certain classes of people. Like minorities. Or dissidents. Or grassroots political movements. *Or anyone who dares think for himself.*

Threat #2 – Militarization has taken over the police. The cops are now using some very nasty weapons. Half the stuff they use is prohibited by the Geneva Convention and the Hague Declaration. The government can't use it in war, but *their own population is fair game*. Modern police technology gives a whole new meaning to crowd control – they use sticky foam laced with chemical irritants. It gives a whole new meaning to interrogation – they use new *mark-free* interrogation tools. And new friendlier, more humane weapons like plastic bullets, pepper gas, and stun guns – that still maim, scalp, burn, mutilate, and kill.

Threat #3 – Big business has taken over proliferation. Any government bureaucrat can buy this stuff. Most of these high-tech gadgets are dual-use. You can use them for benign things like traffic control – or nasty things like people control. Private companies are reaping huge profits manufacturing and exporting this nightmarish technology. Research and development has gone berserk. Who cares

about trivial things like human rights when there's a buck to be made? Heck, if anyone complains just order the $100,000 *mobile execution vehicle* – it comes complete with lethal injection machine, steel holding cell, and areas for "witnesses" and "staff".

Wakeup call...

SPY & COUNTERSPY

This is what our government has been up to while we've been asleep at the wheel. They've been busy making choices. About technology and how to use it. Should technology serve the existing power structure or should it serve the population? Should technology be used to protect the government or should it be used to protect the people?

Well, folks, they decided to protect themselves rather than us. Government for the people is bureaucrat *old-think*. Government against the people is bureaucrat *new-think*. Simply stated, it's hidden-control versus democratic accountability. And hidden-control is winning.

What does all this mean for you and me? Well, it's becoming a lot easier for politicians to use force rather than fix social problems. It's becoming more tempting for them to choose coercion rather than cooperation. Negotiation and compromise are outdated concepts.

Even worse, the new technology makes it easy for them to *disguise* the amount of coercive force they're using.

Put yourself in their shoes. Why go to the trouble of consulting with the people? Why go to the trouble of negotiating with protesters? Why bother listening to dissenting points of view? Instead, all you need do is pick up the phone and arrange their destruction. A few words from the bureaucrat and the *political control apparatus* swings into gear – computerized nationwide surveillance of potential troublemakers, militarized police SWAT teams for demonstrations and meetings, and a friendly salesrep standing by in case government needs more *fiendish devices* for controlling its citizens.

How to make people say yes. When authority fails, repression begins. Eventually terror becomes official government policy. Look around you. Futuristic scenario? Sci-fi thriller? Hollywood's next blockbuster? Nope. *Get real.*

Wake-up call. It's already here. *Stop and think.* Waco. Vickie Weaver. No-knock search warrants. Property confiscation. National identity cards. A cashless society. Across the USA, more and more people worry that *governing-by-authority* has become *ruling-through-repression*.

Governments today can arm themselves with ghoulish toolkits for political control over individuals – and over entire populations. Most people are unaware of the nightmarish systems that technology has made available to bureaucrats. It ain't pretty. And it ain't cheap. But, hey, it's your money they're spending to protect themselves *–from you*.

What is the real problem? The crux of the problem is bureaucrats *who don't like people*. They don't care about people the way you and I do. They only care about themselves – and power. Technology is about to give these *social misfits* the power to exercise absolute political control over entire populations.

The scientists who are providing this technology refuse to accept blame for how their monstrous devices are used. These antisocial *idiot-savants* have created the ultimate Frankenstein's monster – a juggernaut that will make worldwide slavery a reality.

Background – What you need to put this article in perspective. This article is based on information from official sources. Recently the *European Parliament* commissioned a study about political control in today's world. This article is based on that study.

The study was intended as a guide for Members of the European Parliament to inform them about recent developments in technology useful for political control over people. The resulting document, released through the Directorate General for Research, was a political bombshell.

The report first surfaced on 6 January 1998 in Luxembourg as a consultative version of a working document. The original document is a whopping 293KB in size. It is available on the Web at http://www.jya.com/stoa-atpc.htm. A 112-page paper version is available from the European Parliament department responsible, at fax number 352-4300-22418.

Twisted science... New technology for political control over people

This crisis has been about 30 years in the making.

The crisis has been about thirty years in the making. In 1972 the *British Society for Social Responsibility in Science* issued a warning about the emergence of a "new technology of repression". In 1977 a report called *The Technology of Political Control* further described the looming menace.

Britain, with help from its allies, was using the conflict in Northern Ireland as a laboratory. The authorities tested new technologies of repression and control on a large population. They perfected watchtowers built over *underground three-story bunkers* filled with computers that used sonar and infrared technology to *watch people through the walls of their homes*. The arrogant British soldiers couldn't resist gloating – they routinely taunted and humiliated Irish women by describing the undergarments the women were wearing. Keep this in mind the next time you see a snooty British prime minister on TV waxing eloquent about principles. The fact that the IRA was able to operate in such an environment is testament to their countersurveillance and insurgency skills.

The US, with help from its allies, further refined the technology during the Vietnam war and afterwards. Smart bombs. Surveillance satellites. Psychological profiling. Defoliants. Stealth aircraft. Stun guns. Motion sensors. Night vision. Human odor sensors. DNA fingerprinting. Kill fencing. Helicopter-based telephoto surveillance. Laser sights. Repellent electrified panels on crowd-control vehicles. Psychological-based torture techniques.

There has been a dramatic change in the technology of socio-political control during the previous 25 years, especially in the USA, UK, Germany, and France. And yet there has been *no control* over the research, manufacture, deployment, and export of these new technologies. Outdated laws and regulations have simply not kept pace. Much of this new technology is dual-use, so it can be purchased under misleading pretenses. The video surveillance cameras in Tiananmen Square were purchased from a US company as an advanced traffic control system. They enabled China's dreaded security service, the Guoanbu, to identify and arrest *all* of the activists who were demonstrating for democracy.

A new type of weaponry...

The technology of political control is made up of hardware, software, and liveware.

Simply stated, the technology of political control is a new type of weaponry. This technology is used to neutralize the state's internal enemies. In most cases *this means the population*. Most governments today see their own population as the major threat to their existence.

The technology of political control is made up of three components – *hardware, software, and liveware*. Hardware is the apparatus. It consists of instruments, tools, machines, appliances, weapons, and gadgets. Software is the method. It consists of standard operating procedures, routines, skills, techniques, and methods. Liveware is the implementation. It consists of the human element – rationalized human social organizations, arrangements, systems, and networks.

This new technology has created a growing pattern of abuses. It threatens the rights of assembly, privacy, and due process. It smothers freedom of political and cultural expression. It weakens what little protection we have against arbitrary arrest, torture, and *extra-judicial execution*.

What makes this new technology so scary is the people using it. Bureaucrats. Faceless people operating behind closed doors. Unaccountable. Uncaring. Unrelenting.

Even in the so-called democracies, it is the bureaucrat who runs the show. A well-documented phenomenon called *bureaucratic capture* is the cause. Around the world, senior bureaucrats in government control their elected ministers, rather than the other way around. Elected politicians may come and go, but the bureaucrat remains – *as a virtual dictator*. If there is such a thing as a ghoul, surely it is the bureaucrat.

The police-industrial complex. During the 1990s huge sums are being spent on the research, development, procurement, and deployment of new technology for police and internal security forces. A massive *police-industrial complex* has come into being. It is

A massive *police-industrial complex* has come into being. It is similar to the military-industrial complex. Many companies are doing business in this newly-emerging market. There are *huge profits* being made.

From the bureaucrat's viewpoint, all this is good. It increases efficiency and cost-effectiveness. *After all, only those with something to hide resist, right?* To the bureaucrat's way of thinking, the use of so-called minimum force is always justifiable. Existing regulations and controls are satisfactory. After all, technology upholds democracy, they assert.

Well, folks, that's just polite talk for what's really happening. Social conflicts and their participants are either reconciled, managed, repressed, lost, or *efficiently destroyed*. This ruthless application of cold logic is made possible by the new technology of political control – and by a class of bureaucrats who simply don't like people, except for the rich and powerful for whom they act, of course.

Privacy forbidden... New surveillance capabilities

All this technology gives government tremendous power over us.

Life was a lot simpler 40 years ago at the peak of the Cold War. In 1963 the East German security service (the notorious Stasi) used 500,000 informants to monitor and intimidate the population. The Stasi needed a staff of 10,000 agents just to eavesdrop on telephone calls throughout East Germany.

That was then. This is now. Today an entire population can be *automatically* monitored. The trick is to use computers running *word-recognition software*. Every telephone conversation is scanned for suspicious words – if any are found the conversation is stored on disk for a human agent to review at a later time. Today's computers also feature *voice-recognition software*. The security service can tell who is making the call, even if it's from a public pay telephone. Even more unsettling is the newest generation of mapping software. It creates a graphic display – a city map showing locations of *who-called-who*. It makes police roundups a lot easier. (Alas, the more things change, the more they stay the same. 40 years ago the East German security service rounded up dissidents during a so-called *ratissage* – a rat hunt. Today the FBI calls it a *no-knock entry*.)

All this computer hardware and software may seem impressive, but in the USA the National Security Agency continues to push the envelope with self-learning neural network software that uses *human-like* artificial intelligence.

All this technology gives the government tremendous power over us.

Looking for trouble. Today's surveillance apparatus is routinely used by both the government security service and the police. They go on fishing expeditions, looking for trouble that doesn't exist yet – or creating trouble where none exists.

The security service uses surveillance to track dissidents, journalists, human rights activists, student leaders, political opponents, and union leaders. This is illegal, of course.

The police use surveillance for *pre-emptive* policing. They track certain classes of people. This surveillance, identification, and networking results in mass routine surveillance of large segments of the population *without the need for warrants and formal investigations*. This too is illegal, of course.

Huge amounts of low-grade intelligence are created. It is used by the government to monitor certain *social classes* of people and certain *races* of people living in so-called red-lined areas before any crime is committed. Hey, in the eyes of the government, you're automatically presumed to be guilty and deserving of surveillance.

The curse of dataveillance. When computers are employed to tie together unrelated databases for use by the security service or police, it is called dataveillance. In the USA, 700 databases can be monitored simultaneously. A surveillance team has instant access to your driver's license, your marital status, your last credit card purchase, the mortgage on your house, your health records, your employment history, your tax return, political contributions, and a *potpourri* of other personal information.

Combine this information with a network of *closed-circuit television cameras* (CCTV) and you've got an impressive apparatus for population control. So-called traffic-control cameras can recognize vehicle license plates – and *track your movement around*

the city. Cameras in shopping malls, retail stores, fast food outlets, parking lots, and other public places can track you on foot.

When this network of surveillance devices is tied together by computer networks, it results in pre-emptive policing. The system targets certain classes of people rather than specific types of criminal activity. Much of the surveillance apparatus is automatic. It runs on artificial intelligence.

Now it starts to get scary. Here's why. This massive apparatus of surveillance and repression can be easily be refocused and retargeted if the political environment changes. Even in the world's so-called democracies, all it takes is a word from the nation's leader to declare a national emergency and implement special measures (this is polite talk for *setting up a dictatorship*, folks). Just stop for a moment and imagine living under a dictator equipped with such enormous capabilities of surveillance, repression, and control over the general population. Hitler and Stalin were a couple of *milquetoasts* compared to what's coming next.

What we're talking about here are huge police databases and widespread abuse of civil liberties. Systems like this are usually first forced on groups with little political power like welfare recipients, the unemployed, and minorities. If they complain about invasion of privacy, no one listens. Then, as the oppression begins to be accepted, the dataveillance system is *expanded up the socio-economic system*.

The potential for abuse is so great that legislators in Denmark have banned CCTV systems. But it's the only country in the world to do so. Some legislators in Europe were so alarmed that they passed Article 15 of the 1995 *European Directive on the Protection of Individuals*, which grants everyone the right "not to be subject to a decision which produces legal effects concerning him which is based solely on the automatic processing of data". Automatic video-camera speed-traps are making a mockery of that legislation. (I am embarrassed to admit that a key manufacturer of this new radar-trap technology is actually located in the city where I live.)

The core issue. As few as 20 years ago, personal information about each us was fragmented. It was stored in many separate, unrelated locations. It was extremely difficult to acquire and collate. That's where the safety factor was. But it's gone now. In today's world, networked computers make retrieval easy. Cross-referencing and collating is a snap. Simply stated, it is *bureaucratic heaven* for the unelected, sociopathic, control-freaks that run the system.

Biometric systems. The spread of computer-driven biometric systems promises even greater loss of individual privacy. What we're talking about are devices like automatic fingerprint readers and *human identity recognition systems* that analyze characteristics like genes, odor, signatures, and the pattern of capillaries at the back of the retina. For example, databases of DNA fingerprints are popular with police in Britain. The data is already being used to justify pre-dawn raids of large groups of suspects in the UK. Even more disturbing, face recognition systems are being tested in the USA, France, and Germany. In a few short years, you can expect FBI SWAT teams to be kicking in doors at 5 am simply because *some computer program* has concluded that your facial characteristics may match the description given by some sleazy informant under duress by his FBI handler.

Other goodies for bureaucrats. Bureaucrats and their toadies can choose from a well-stocked toolkit of surveillance and oppression gadgets. Night vision systems. Recognition and tracking of human heat signatures in total darkness. Helicopter-based telephoto surveillance. Passive millimeter wave imaging *that can see through clothing* – this will add a new dimension to airport pre-flight screening areas.

In today's world, electronic bugs are disguised as light fixtures, telephone packages, telephones, clocks, cable-TV decoders, even *cockroaches*. Multi-room monitoring systems are becoming popular with both the police and the government security service. And *low-intensity magnetic pulse tools* can be used to momentarily disrupt your thinking and confuse you.

A number of companies are currently selling converted notebook computers than can eavesdrop on all cellular telephone conversations in a given area. The software is compatible with Windows 95. Simply scroll down the menu and click on the number(s) you want to listen to.

The interception networks...

The scope of the system is mind-boggling. For example, all email, telephone, and fax communication is *routinely intercepted* by the NSA in Europe, USA, Central America, South America, Canada, and Mexico.

Project Echelon taps into the system of Intelsat satellites and the world's long-distance telephone calls, Internet communications, email transmission, faxes, and telexes. This is a billion dollar intelligence-gathering network. It is used by NSA to monitor everything from dissidents to the activities of international banks. Data processing sites are located at Yakima (USA), Wailhopai (New Zealand), Geralton (Australia), Hong Kong, and Morwenstow (UK). Other countries like Canada and Germany are also key participants in the data-gathering scheme.

Whistleblowers inside Project Echelon are claiming widespread abuse, including malpractice and negligence. Even Amnesty International is routinely surveilled by the spooks.

Not to be outdone, the European Union (EU) is in the process of setting up its own massive eavesdropping network.

A call to action... How to save yourself

It's worth saying again. It was important enough to say it at the beginning of this article – and it's important enough to repeat.

You're about to lose something. It's already slipping from your grasp. And once it's gone, you'll never get it back.

As a people, we are facing the most serious threat to humanity in recorded history – the systematic stripping away of traditional freedoms by governments worldwide. And that includes *all* governments.

It is a situation far more serious than the plagues of the Middle Ages that nearly wiped us out as a species. It is a threat never before seen in ten thousand years of human history.

You are about to become the property of the government.

A call to action – How to save yourself. A hundred years ago, privacy was taken for granted. It took a lot of time and effort for the authorities to invade your privacy.

Today the situation is reversed. Surveillance is the norm. The technology of political control has made it very easy for the authorities to watch you. It takes deliberate effort by you to enforce your right to be left alone. In today's world, you must earn the right to privacy. By doing nothing, you forfeit your privacy – and your life becomes an open book. Any bureaucrat can watch you.

What can you do? *Be aware of what's really going on.* Quietly resist. In your own way, work against the dehumanizing political control that government is trying to implement.

Learn countersurveillance skills. Protect what is left of your freedom. Learn activist tactics and go underground if you feel you have to. *But act soon.* Wait much longer and it may be too late. For some people it may already be too late. Return to our home page for more sources of information about countersurveillance and the basics of underground activist tactics.

Coming up next...

Coming next in Part 2 of the Bureaucrat's Toolkit. The next installment of Bureaucrat's Toolkit will explore *crowd-control* technology and *prisoner-control* technology.

Human pain – New crowd-control weapons. You'll learn about new paralyzing weapons – as well as chemical, kinetic, and electrical weapons – rubber bullets, plastic bullets, and beanbag projectiles. You'll find out about discrete-order vehicles like *pseudo-ambulances* that hide SWAT teams inside – and crowd-control vehicles with a retaliatory capability like *repellent electrified panels*. You'll see how these vehicles seal people *inside* a zone rather than chasing them out. You'll learn how police dum-dum ammunition can amputate your arm or leg – without immediate medical attention this amounts to an extra-judicial execution. You'll learn about mark-free torture methods – the authorities no longer fear embarrassing questions from Amnesty International – because *you can't prove you were tortured*.

Human warehousing – New prisoner-control technology.

You'll see how government plans to cut expenses by replacing staff with technology. You'll learn about the social implications of a strategy of human warehousing rather than rehabilitation. You'll learn about *kill fencing*, lethal area-denial systems, and electric-restraint technology. You'll see how heavily private industry is involved – electrocution systems sell for $50,000 – a gallows sells for $85,000 – and you can pick up a mobile execution vehicle with lethal injection machine for a paltry $100,000. You'll also learn how *psychotropic drugs* are used to control prisoners. You'll discover laser sights and silencers that make it easier to implement extra-judicial execution – as well as synchrofire systems that provide *push-button control* over firing squads.

Where do you go from here?

The keys to success in today's world of unregulated surveillance are twofold – knowledge and skills. First, you need knowledge of your adversary's capabilities. Second, you need skills in the art of countersurveillance. You can get both by reading *Spy & CounterSpy*. In fact, that's the only way you can get them.

Back to Home Page

techniques or the documentation contained in this product. The author and publisher shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of the techniques, associated instructions, and/or claims of productivity gains.

How to organize a resistance movement...

SPY & COUNTERSPY

If you agree that life, liberty, and property should be the right of every citizen, then you probably already realize that surveillance and suppression by government goon-squads is incompatible with these three basic human dignities.

Getting involved. Organizing and activating your own *resistance movement* can be an exciting and rewarding experience – especially if you yearn to do something meaningful about the unfairness you observe around you every day.

Like the heroes and heroines of the American revolution, you may choose to answer the call to *idealism and sacrifice*.

If you love your country but fear your government, becoming an underground activist may give you the mechanism you need to start making a difference.

Becoming aware. As the saying goes, freedom is sustained by three boxes – the *ballot* box, the *jury* box, and the *ammo* box. Unfortunately, more and more concerned citizens are becoming increasingly alarmed by what they see as the dangerously *weakened condition* of the ballot box and the jury box.

Reliable sources. The article you are reading is based on information obtained from our contacts in a number of resistance movements. The information in the article is also based on official *counter-insurgency training manuals* leaked by our contacts in intelligence agencies and security services.

This article is intended as *an introduction* to organizing and activating a resistance movement. Other articles and tutorials at our Web site can provide you with *hands-on skills*.

Step 1: Create your commando...

1. Become focused. Get a sense of direction and purpose. Create a leadership team. Develop a strategic plan, an order of battle, or a manifesto. Start building the commando leadership cadre. As the saying goes, *plan your work* and then *work your plan*.

2. Become invisible. Go underground. Create an identity that cannot be traced, located, or discovered by the authorities. Adopt a *nom de guerre*. Become independent by being self-funding and self-supporting. You can continue to live your normal life if you wish, but you must have an underground persona for your resistance work. Your normal life can provide cover for your underground life.

3. Set up communications. Establish secure methods for one-way communications. You'll need to communicate with the population, with the media, with the authorities, with other cells, and with other resistance movements. Set up anonymous cyber-cafe email accounts. Set up dead-letter boxes in your neighborhood. Acquire anonymous prepaid calling cards for telephone communications. Develop skills in elliptical conversation.

4. Recruit members. The longer you've known them, the better. Encourage them to establish *cells*. Whenever a cell has more than ten members, divide the cell. Then form *circles* from groups of cells. Appoint circle leaders. Communicate with the circle leaders (but also maintain some direct links to individual cells for sensitive operations). Form *sections* from groups of circles. Appoint section leaders.

Step 2: Become active...

1. Begin propaganda. Inform your cells about the misinformation campaigns of the authorities. Also inform the general population. The authorities will spread lies about you, about your group, about your motives, and about your actions. This is *standard operating procedure* for a corrupt and repressive

government.

2. Begin defensive operations. Assist persecuted persons by warning them, by hiding them, or by providing escape routes. You can also assist persecuted persons by publicizing the repressive actions of the government's goons. Expect the goons to react.

Each person in the general population will fall into one of six possible categories – activist, supporter, sympathizer, undecided, collaborator, or traitor.

3. Begin political operations. Inform the general population about how to behave towards the authorities. For a typical resistance movement this may include civil disobedience, non-fraternization, protest, non-cooperation, and so on. Each person in the general population will fit a profile – *activist, supporter, sympathizer, undecided, collaborator, or traitor*. A government's terror campaign of no-knock warrants, confiscation of property, national ID cards, secret internment camps, corrupt officials, etc. will move people's attitudes along this continuum. Most people will start out undecided – you want to convert these people into sympathizers, supporters, and activists.

4. Begin counterintelligence operations. Isolate informers, agent-provocateurs, moles, passive-aggressive types, toadies, collaborators, cowards, honeypots, and so on. Ostracize these individuals so they cannot damage your resistance movement. Instruct the general population to shun these individuals. Distribute their identities and modus operandi to all cells.

Step 3: Begin guerrilla operations...

1. Go on the offensive. This may involve lawful action like protest, civil disobedience, tax resistance, a letter-to-the-editor, work slowdown, embargo, consumer boycott, agitation, *silent* non-cooperation, *noisy* non-cooperation, unprovable minor acts of sabotage disguised as oversight or accident, ostracizing employees of government agencies, setting up alternative self-sufficient communities, and so on. In addition, however, a typical resistance movement in today's world often undertakes unlawful operations like terror, sabotage, assassination, and seccession.

2. Enforce cooperation. A resistance movement will often need to use *counterterror* to intimidate traitors, collaborators, and informers. The goal is to make it dangerous to cooperate with the authorities.

About your long-term strategy...

According to the official *counter-insurgency training manuals* of various intelligence agencies and security services, a successful resistance movement always follows the same sequence of events.

First comes passive resistance. This eventually leads to active resistance, which in turn leads to guerrilla operations. This escalates to open insurrection by insurgents – which inevitably results in civil war.

A typical successful resistance movement goes through phases – passive resistance, active resistance, guerrilla warfare, open insurrection, and civil war.

This process can be interrupted at any stage by a government willing to make concessions to the population. Unfortunately, however, the antisocial bureaucrats behind repressive governments are rarely willing to compromise on their policies.

Strategic resistance. A typical resistance movement uses both active *and* passive resistance until the situation deteriorates to a point when *urban guerrilla warfare* can be initiated.

Guerrilla warfare. As the situation becomes more volatile, a typical resistance movement uses *hit-and-run* guerrilla tactics until *open insurrection* can be initiated.

Insurgency. As the government begins to lose control of significant elements in the country, a typical resistance movement will use the insurrection to provoke civil war. It then uses civil war to force *fundamental change* in society.

SPY & COUNTERSPY

Spy school for the rest of us.

Back to Home Page

Here is the small print. It appears here because we have found that maintaining a corporate front is the only way we can protect ourselves against interference by governments and their agencies. The legal underpinnings of our corporate front are our first line of defense against audit-attacks and other methods of economic warfare that the authorities use to suppress dissent, protest, and activism. They are also determined to prove their hypothesis that *Spy & CounterSpy* is funded by a foreign intelligence agency or terrorist group – but our double entry accounting record of corporate revenue and expenses is our shield against fabricated evidence by an overzealous investigator or case officer.

Lee Adams Seminars is a division of Here's-how, Right-now! Seminars Inc.
OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com
EMAIL ENCRYPTION: Click on *Ask Agent X* for our public key.

Secret Meetings

Tradecraft for managing clandestine contacts...

A security service like the FBI can only achieve its objectives by intercepting communication between people. This means you can beat the security service if you can deny them the ability to overhear your meetings with your contacts.

What you'll learn here...

This article teaches you how to check for surveillance before you meet with a clandestine contact. You'll learn a protocol that will beat security services like the FBI, BATF, DEA, and others. The method is particularly effective against standard police surveillance. It also works against the so-called *inspection teams* of the IRS.

Tradecraft origins. The method described in this article was originally devised in 1943-1944 by countersurveillance expert Anthony Blunt for Britain's MI.5. Unfortunately for the British, Blunt was a deep-cover agent for the KGB.

Six years later, Blunt taught the protocol to his new KGB controller, Yuri Modin. Together they perfected the technique as it is known today. They successfully thwarted MI.5 surveillance for three years, sometimes even meeting *daily* to exchange information and top secret documents. In effect, Blunt was using his *inside knowledge* of MI.5's surveillance techniques to beat them at their own game.

Proliferation. This countersurveillance method has since been adopted by Israel's Mossad, Germany's BND, Russia's KGB (now the SVR), the American CIA, and many others. The protocol is taught by intelligence agencies to their controllers – these are the intelligence officers who manage and meet with deep cover agents in foreign countries. The method is also being used today by resistance movements and urban guerrilla groups.

When this countersurveillance protocol is methodically applied, it is extremely difficult for a security service to breach your security.

Step-by-step instructions...

Here's a hypothetical situation. Assume that you and I wish to meet clandestinely. We wish to ensure that our meeting is not observed by a surveillance team.

You and I have previously agreed upon a place, date, and time. In addition, we are familiar with each other's appearance – we can recognize each other on sight.

Step 1

You and I independently arrive at the previously agreed-upon *general* location. Rather than fixing a specific location, we agree to be only in the *general vicinity*. This is an important principle.

This might be a large park, a residential district, etc. The location must be outdoors and free of video surveillance cameras. It should also be selected with the intention of thwarting telephoto lenses.

You and I should each know the area well. The location should provide reasonable cover for each of us being there – strolling in the park, walking through a residential area to a bus stop, convenience store, etc.

Step 2

You and I will eventually make eye contact at some distance from each other. We do this discretely, so others are unaware. I use a pre-arranged signal to alert you that I have spotted you. Perhaps I'll throw my jacket over my shoulder, or remove and clean my sunglasses, etc. The signal must be a natural movement that does not attract unwanted attention.

Safety first. Even though you and I have seen each other, we do NOT approach each other. This is an important safety valve. If

either of us has *grown a tail* we do not want to compromise the other person.

BACKGROUND – The phrase *grown a tail* is spy-talk for being under surveillance. The phrase is somewhat inaccurate, because they don't just follow you, they often surround you.

Step 3

When you see my signal you simply walk off. Then I follow you in order to ensure that you're not being watched. I carefully check for the presence of a *floating-box* foot surveillance team. I check for agents at fixed *observation posts*. I also watch for *drive-by* support from a floating-box *vehicle surveillance* team.

BACKGROUND – In particular, I may follow you, I may walk parallel to you, I may occasionally walk ahead of you. The goal is simply to be nearby so I'm in a position to detect surveillance around you. I always remain at a distance from you, of course, never approaching too closely.

Step 4

When I have satisfied myself that you are *clean*, I again signal you. Perhaps I re-tie my shoe laces.

Step 5

Now we reverse roles and this time it is I who simply walks off. You begin to follow me in order to ensure that I'm not being watched. You check for *floating-box* foot surveillance, fixed *observation post* foot surveillance, and *drive-by* support by a vehicle surveillance team.

What to look for. You carefully watch for persons who are pacing me or moving parallel with me. You check for persons loitering at positions with a good *line-of-sight* to my location. You watch for an *ongoing pattern* of people coming and going that results in *someone* always being in a position to monitor me. You watch for vehicles dropping someone off ahead of me.

Step 6

When you are satisfied that I am *clean*, you signal me that I'm not being watched. (On the other hand, if you suspect that a surveillance team is in the vicinity, you simply abort the operation and walk away.)

BACKGROUND – You must trust your instincts, because if something seems *not quite right* it's better to be safe than sorry. Many people are surprised to learn that it is not difficult to detect a surveillance team watching someone else. This is the subtle elegance of Blunt's countersurveillance system. And the goons are helpless against it.

Step 7

You and I can now approach each other and meet. After our discussion we agree upon the date, time, and location of our next clandestine meeting – as well as two backup plans in case the meeting is thwarted by surveillance. If we are unable to meet at the first venue we will use our fallback position and we will meet at the same time and place one week later. If we are unable to make that meeting happen, we will shift to a previously agreed-upon failsafe plan and we will meet at a *different location* at an agreed-upon date and time.

Neither you nor I writes down the particulars of our next meeting. We commit the details to memory.

BACKGROUND 1 – If you have any documents to give me, I will not accept those documents until the final moments of our meeting. I will have already started making my *getaway* when I accept the documents. This reduces the chance of discovery and arrest by a surveillance team that has managed to elude our countersurveillance protocol. If the security service acts too quickly, they will have no evidence against me, because the documents have not yet been passed to me.

BACKGROUND 2 – The best agents never mix discussion and documents. If a document is to be passed, no discussion occurs. The entire contact takes only a moment – the perfect brushpass. The principle is simple. It is foolhardy to stand around holding incriminating documents.

Spook talk...

Spies in North America call this seven-step protocol for countersurveillance *drycleaning*. In Europe, it is called *parcours de s餸rit鐳i> – a French phrase which can be translated as security run or security circuit*.

Spy school for the rest of us.

http://www.SPYCOUNTERSPY.com

Back to Home Page

Here is the small print. It appears here because we have found that maintaining a corporate front is the only way we can protect ourselves against interference by governments and their agencies. The legal underpinnings of our corporate front are our first line of defense against audit-attacks and other methods of economic warfare that the authorities use to suppress dissent, protest, and activism. They are also determined to prove their hypothesis that *Spy & CounterSpy* is funded by a foreign intelligence agency or terrorist group – but our double entry accounting record of corporate revenue and expenses is our shield against fabricated evidence by an overzealous investigator or case officer.

Lee Adams Seminars is a division of Here's-how, Right-now! Seminars Inc.
OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com
EMAIL ENCRYPTION: Click on *Ask Agent X* for our public key.

Handling the everyday risks of leading a double life...

The heroes and heroines of the American Revolution held the deep conviction that everyone everywhere has *the right* to revolt against tyranny and oppression.

Many Americans today are wondering if they should become active in resisting government tyranny. Some are asking themselves, *Do I love my country but fear my government?*

Answer one question and you've answered both.

The element of risk

Is there risk involved? Yes. Anyone who questions or challenges the status quo is a target for surveillance and repression by the authorities. Anyone who undertakes covert actions must accept an even greater risk.

Your primary duty as an underground activist is security. You must remain unknown to the adversary's forces – and to the public at large. Simply stated, *exposure* is the greatest threat you face as an underground activist or as an urban guerrilla. This risk falls into three categories.

Sources of risk

Commonplace, everyday situations are the main source of risk. Many people are surprised to learn this. The three main causes of exposure are

first, *being in the wrong place at the wrong time* (when the police are looking for someone else);

second, *being noticed by the security service* (while they're watching someone else); and

third, *being reported to the authorities* (by a busybody or a nosy neighbor).

Reduce or eliminate these three situations and you've removed 98% of the danger in leading a double life.

What you'll learn here

This article teaches you how to minimize the risk of the double life you must lead. The article contains enough background information to keep you out of the internment camps. Combine it with the other tutorials at our website, and you'll know enough to begin planning and carrying out covert actions.

Threat #1 – The wrong place at the wrong time...

The threat involves being inadvertently and innocently swept up in an investigation. You're simply in the wrong place at the wrong time when the police are looking for someone else. When you're this close to them, arouse their interest and you're finished.

Situations can develop around you unexpectedly. They can get out of control even quicker. They include mundane events like random vehicle stops by police. More serious situations include muggings, holdups, shoplifting, drunk-driver road checks, prowlers, burglaries, retail video cameras, and others. All of these situations will bring the police close by.

Here's an example.

Case Study #1. October 1998 – I was scheduled to meet a clandestine contact. The location was the entrance to a city park just after dark. I arrived ten minutes early in order to give myself time to check for surveillance.

The park is laid out as a linear trail. It meanders through various neighborhoods in the city. Unknownst to me, just moments earlier a punk had held up a nearby convenience store. He used the trail for his getaway.

I parked my car, walked to the meeting location, and checked for surveillance. Satisfied that the area was clean, I was walking

for surveillance. Satisfied that the area was clear, I was walking back to my car. Suddenly, out of nowhere, a large dark sedan pulled out of the shadows. A male got out of the car and crept along the dark side of a building adjacent to the park. He hadn't seen me. I was thinking perhaps it was a prowler, burglar, or drug-related situation.

A challenge in the dark. As I approached my car, the suspicious male shone a flashlight on me. He was about 25 yards away. Using a firm voice, I challenged him, *"Can I help you with something?"*

"It's the police."

"Oh, sorry," I called back. *"I didn't recognize you."*

I started walking towards him in a nonthreatening way as if I had nothing to hide.

Sitrep. I had a number of things going for me. I was well-dressed. I was wearing a sports coat and tie – somewhat overdressed for the park. And I had just reacted in a manner that suggested I was not going to accept being challenged by a stranger in the dark. All these factors may have reduced the cop's suspicions a bit. As he and I approached each other in the dark, he came right out and told me that he was checking the park as a possible getaway route of the robbery suspect.

I played my cover and began acting worried. *"Gee, thanks for the warning. I was just in there."*

Summary. Picture it in your mind. It's just him and me. On a deserted street. In an industrial area. After dark. He's all *pumped up* looking for an armed robbery suspect. It wouldn't take much for things to get out of hand.

His next move. Following standard police procedure, he now needed to rule me out as a suspect *and* find out what I was doing. After all, here I am hanging around a park after dark.

He asked for identification. I showed him my driver's license. Then he asked what I was doing.

"I'm going down to [name of bar] to sing some Karaoke," I replied, looking at my watch. It was twenty to nine.

"It doesn't start 'til nine," I continued. *"So I'm just killing a little time."*

He smiled. Then he handed back my ID and he said, *"Well, you're not 24. Have a good night."*

Home free. We can safely assume the robbery suspect was described by the convenience store clerk as a 24-year old male. I'm fortyish.

The lesson? You simply never know when circumstances are going to overtake you. You cannot predict when you're going to be challenged by the authorities.

Plausible denial is the best way to ensure that a routine challenge doesn't escalate into a major confrontation. As an underground activist, you *must* have an innocent explanation for *everything* you do. In my case, I also had a *backstop*, which is spy-talk for an actual event that backs up a cover story.

Tell the cops what they want to hear. Help simplify their job for them. Play your cover for all it's worth. Be a stereotype. Make it easy for them to label you, to pigeon-hole you, to typecast you – and they'll rule you out as a suspect.

I was just some naiive *dandy* on his way downtown to sing Karaoke on a Saturday night.

Yeah, right.

Give them what they want. An important component in your plausible denial and your cover is to give the authorities something to *"find"*. Let them discover a personal character weakness or a minor transgression. They'll seldom look further. Intelligence agencies like Britain's MI.6, Germany's BND, France's DGSE, and Russia's KGB (now SVR) have been doing this for decades. It's called *layered security*.

The damage? None. I simply rescheduled my rendezvous with my contact, a whistleblower in an alphabet agency.

Summary

Threat – Unexpected police challenge.
Defense – Plausible denial. Good cover. Layered security. A backstop.
Implementation – Dress well. Be clean and neat. Be polite. Play out your cover. Become a stereotype. Act nonthreatening.

Threat #2 –
Being noticed by the security service...

The threat involves being noticed by the security service when they are actually watching someone else. In other words, you inadvertently walk *through* a surveillance operation.

During your meetings with various contacts, eventually you'll find yourself talking to someone who is under surveillance. The surveillance team will want to know more about you. The mere fact that you've contacted their target is enough reason for them to place you under surveillance.

They don't have anything on you yet, but the situation is extremely dangerous for you.

A common trap. A situation lke this can easily develop as a result of your routine interaction with other activists, urban guerrillas, cells, networks, couriers, go-betweens, suppliers, informants, whistleblowers, agent-handlers, and so on. Any one of these conctacts might be under surveillance – vehicle, foot, or technical.

The defense against this threat is to use good tradecraft.

Use the *Blunt-Modin* method of arranging secret meetings. Return to our home page and click on *Arrange secret meetings* for more on this.

Use DLBs. Return to our home page and click on *Use dead-letter boxes* for more on this.

Use anonymous email accounts. Return to our home page and click on *Be a whistelblower* for more on this.

Use one-time pads. Return to our home page and click on *Use a one-time pad* for more on this.

Learn to recognize the warning signs of surveillance. See various articles at our website, including *FBI vehicle surveillance* and *Beating the FBI*. Other articles and tutorials are coming soon.

Use elliptical conversation. Use diversions and decoys. Use misinformation. All these skills make it possible for you to continue your underground work while under surveillance. Most important, however, is your *cover*. You want to appear as one of the unthinking sheep. Make yourself uninteresting to the surveillance team.

Failsafe. Even if you don't detect the presence of the surveillance team, *good tradecraft* and a *good cover* will keep you free. The goons will watch you long enough to satisfy themselves that you're not a suspect – and then they'll move on. The cardinal rule is *don't break cover*. Ever. Let them hear what they want to hear – *a sheep bleating*. Let them see what they want to see – *a sheep grazing*. Help them rule you out as a suspect.

Here's an example.

Case Study #2. July/August 1998. One of my regular contacts was under intermittent police surveillance. That's because she has occasional contact with nasty underworld types. She and I discussed *nothing* by telephone. We use only *random* parks and noisy bars for our conversations. Sometimes we used cutouts and go-betweens to pass messages to each other and set up meetings.

The cover? I was just a naiive *dandy* who was hopelessly infatuated with a *"bad girl"*.

Yeah. Right.

Layered security. As in the previous risk analysis, it's important to realize that an essential element in your plausible denial and your cover is to give the authorities something to *"find"*. Let them discover a personal character weakness or a minor transgression. They'll seldom look further. Intelligence agencies have been doing this for decades... because it works.

Summary
Threat – Noticed by security service.
Defense – Good tradecraft. A credible cover. Layered security.

Threat #3 –
Being reported to the authorities...

The threat involves being reported to the authorities by a busybody or a nosy neighbor. These so-called *anonymous tips* happen a lot more often than people realize. The threat is from the passerby, the bystander, the witness, the jilted lover, the jealous coworker.

This is one of the most dangerous threats to your double life, but it's also one of the easiest threats to neutralize.

The answer? Good cover and plausible denial. This means looking like *you belong* – and having an innocent explanation for whatever it is you're doing.

Your public persona must provide adequate cover for the activities of your underground persona. Of course, this only works if you keep your mouth shut. Don't brag about your activities to friends or lovers. Don't engage in *pub talk*. Unless you're among cell members, keep your political opinions to yourself.

Case Study #3. The research that I undertake during my investigative reporting for the *Spy & CounterSpy* website provides good cover for the *"serious"* contacts I need to make. My research activities provide plausible denial while I meet or communicate with informants from alphabet agencies, whistleblowers from government departments, activists in underground organizations, confidential sources in law enfourcement and the media, tipsters, ex-military types, ex-spooks, and so on. What we *really* talk about is between me and my contacts, of course.

With a little thought you can exploit *or create* activities in your lifestyle that provide good cover for the things you'd rather be doing.

Summary

Threat – Reported to the authorities.

Defense – Good cover. Be part of the community. Fit in. Be friendly. Be a stereotype. If possible, have a solid backstop.

SPY & COUNTERSPY

Spy school for the rest of us.

http://www.SPYCOUNTERSPY.com

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com

How to set up and use a dead-letter box...

SPY & COUNTERSPY

This article describes how deep-cover agents pass messages, documents, money, weapons, and other material between each other – without compromising their security. Neither agent knows the identity of the other. Nor do the authorities know what's going on.

The method described in this article has been used by foreign intelligence agencies and underground groups to thwart the counterintelligence and counterespionage sections of the FBI.

What is a DLB? DLB is an acronym for dead-letter box. It is also called a dead drop. A DLB is a physical location where material is covertly placed for another person to collect without direct contact between the parties.

Good locations for dead-letter boxes are nooks and crannies in public buildings, niches in brick walls, in and around public trash receptacles, in and around trees and shrubs, a third-party's mail box, between books in a public library, inside the paper towel dispenser of restaurant washrooms, and so on. The key to success is ingenuity. If the item being passed can be disguised as a discarded candy wrapper or hidden inside a cigarette butt, etc., so much the better.

DLB Protocol. The method described in this article was originally devised and perfected by the KGB for use in Britain and the USA during the cold war. But the technique is so effective it's still in use today – and is used by more than 30 intelligence agencies and underground groups worldwide.

When used by two people who have basic skills in countersurveillance, this method will confound an FBI surveillance team – as demonstrated by the FBI's inept handling of the cases involving Aldrich Ames, Jonathan Pollard, and John Walker Jr.

Tradecraft. You need to know three pieces of tradecraft to make this technique work.

Trick #1 – Pick a good site for your DLB. This means choosing a spot where you're *momentarily* hidden from view while you pass by (and either load or empty the box). It also means selecting a site that is easily accessible and in a public location.

Trick #2 – Use a separate set of sites to signal to your opposite number that you're ready to place something in the DLB, or retrieve something from the DLB.

Trick #3 – Use a foolproof signal that tells both parties that the material in the site has been picked up. This guarantees that the first agent can go back and recover the items if the second agent is unable to make the pickup for some reason.

Step 1: The *ready-to-fill* signal...

Be sure to use a *ready-to-fill* signal that can be easily seen by a lot of people.

Let's suppose that you need to deliver a document to your contact. The first thing you do is transmit a "ready-to-fill" signal. You need to tell your contact that you're ready to fill the DLB with your material.

For example, you might place a piece of chewing gum on a lamp post at a pre-arranged location at a pre-arranged time (perhaps the second Tuesday of each month at 1:30 pm).

The trick is in using signals that can be easily seen by a lot of people. This means that your contact does not have to compromise his/her security while reading your signal.

Step 2: The *ready-to-pickup* signal...

Don't fill the DLB until you see the *ready-to-pickup* acknowledgement

When your contact sees the *ready-to-fill* signal, he/she will send a *ready-to-pickup* signal. Again, this signal must be sent at a pre-arranged time and location, say at 2:00 pm. It might be a chalk-mark on a traffic signpost or back of a park bench.

When you see the *ready-to-pickup* acknowledgement, you must fill the DLB within 15 minutes (ie by 2:15 pm). After placing

your materials in the DLB, you immediately return and remove your *ready-to-fill* signal, thereby indicating to your contact that the box is filled.

Step 3: The *all-clear* signal...

When you see the *all-clear* signal, you can leave the area. If you don't see the signal, return to the DLB and remove the material.

Upon seeing that your *ready-to-fill* signal has been removed, your contact goes to the DLB and retrieves the material that you've placed there for him/her. This must be accomplished before a pre-arranged deadline, say 2:30 pm. Your contact then returns and removes his/her *ready-to-pickup* signal, indicating that the box has been emptied.

When you see this all-clear signal, you leave the area. However, if you don't see the signal by a pre-arranged time, you return to the DLB and retrieve the material in order to prevent it from falling into unauthorized hands.

This system of signals can be made even more secure by using positive acknowledgement signals instead of simply removing existing signals, of course.

Providing security for your DLB...

NOTE – The FBI does *not* want you to know this.

Weave a number of *fake* DLBs into your routine on a daily, weekly, or monthly basis.

To maintain watertight security for your DLB, simply weave a number of *fake* DLB locations into your routine on a daily, weekly, or monthly basis. Narrow passageways between buildings, covered pathways in public parks, nearby dumpsters behind restaurants... all these are ideal.

Simply make it a point to walk past these fake DLBs *on a regular basis*. Remember, each DLB is located such that you'll be *momentarily hidden from view* as you pass it. If you're under surveillance, the goons will go ballistic. They'll need to place an agent at each suspected DLB *at the precise moment you walk by*.

If you've chosen your sites carefully, there's no other way for the goons to monitor these locations. If you have three or four fake DLBs that you regularly walk past, you'll soon notice the *telltale pattern of strangers* who just happen to be loitering nearby at the instant you're momentarily hidden from general view. When this happens, you've detected the presence of a surveillance team. Suspend your covert activities until the surveillance passes.

SURVIVAL TIP – Even if you're not using DLBs, it's a good idea to walk past fake dead-letter boxes as a part of your weekly routine. I've caught more FBI gumshoes than I can count with this one simple countersurveillance technique. To date the FBI trainers have been unable to develop a defense against this particular countersurveillance maneuver – and you just haven't *lived* until you've seen the facial expression of an FBI spook who suddenly realizes he's been *made* by the target of the surveillance operation.

SPY & COUNTERSPY

Spy school for the rest of us.

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.

EMAIL: reader_service@SPYCOUNTERSPY.com
EMAIL ENCRYPTION: Click on *Ask Agent X* for our public key.

How to broadcast to a group of cells...

SPY & COUNTERSPY

Any security service – including the FBI – relies upon intercepted communications to penetrate and ruin an underground movement.

A resistance movement must adopt a professional approach to communicating with its cells – otherwise the FBI will eavesdrop on the group's communications, identify key members in the movement, and begin to infiltrate agents into the organization. Soon the cells are paralyzed by moles, informants, agent-provocateurs, and honeypots.

Return to our home page and click on *Glossary* for definitions.

The Alternatives. For one-on-one communication, you can use a dead-letter drop, also called a DLB. (Return to our home page and click on *Use dead-letter boxes*.)

DLBs are a safe and secure method for passing messages, documents, money, etc. between two people with no contact between the parties. However, they are best suited for intermittent communication between individuals. They are not suitable for broadcasting a message to a group of cells.

Other possible methods include telephone calls from one pay phone to another, newspaper classified ads, bulletin boards in shopping malls, and so on.

Unfortunately, each of these methods involves unacceptable security risks. Pay phone to pay phone communication forces you and your cells to be at a specific location at a specific time, which is inviting detection by the authorities. Newspaper classified ads are routinely monitored by the FBI, BATF, CIA, and NSA – that's why this system is seldom used any more by intelligence agencies or underground organizatons. Bulletin boards require each of your cells to *break cover* by appearing at a specific location.

The Solution. The best solution is for the resistance movement to *piggyback the message* on a transmitter that is already being used legitimately in the community. Examples of broadcasting transmitters than can be utilized are pager systems, local radio stations, local TV stations, cellular telephone networks, courier companies, taxi companies, repair companies with radio-controlled fleets of trucks, and so on.

This article describes a time-proven method that is being used successfully by intelligence agencies in Europe and the USA – as well as underground organizations like the Red Brigades, the IRA, and the Tupamaros. The method entails using an existing paging system without the knowledge of the pager company or its customers.

Step 1: Locate a transmitter...

1. Acquire a scanner. Scanners are readily available at various electronics stores. They can be purchased off the shelf. No license is required to operate a scanner in most jurisdictions. The user's manual provides all the information that a novice needs to become proficient in using a scanner. Many salespersons, eager to make the commission on the sale, will clandestinely slip the buyer a copy of local frequencies (air control, taxi, ambulance, weather, etc.).

Scanners are readily available and no license is required in most locations. The user's manual tells you all you need to know.

2. Find a frequency. Identify one or more frequencies being used by pager services. The messages will often consist of simply a name and number to telephone. For example, *"Dr. Name please call Records at nnn-nnnn"*.

Doctors, paramedics, lawyers, executives, repair personnel, building contractors, and many others use pagers.

The system works like this – a caller who wants a doctor to call back simply telephones the pager company's number, enters a four-digit pager ID number, and speaks a short message. The

pager company's computer records the message and broadcasts it on the appropriate frequency to the doctor's pager unit.

3. Monitor the frequency. The goal is to obtain the names and telephone numbers of callers who are paging someone to call them back. The resistance movement may need to scan at different times during the week to obtain a good sampling. A single frequency may service dozens of pager customers. An embedded code is used to alert the particular pager unit being addressed.

Step 2: Acquire the access codes...

1. Role playing. For the purposes of this article, imagine you're an urban guerrilla. You telephone one of the callers whose name and number you've acquired with your scanner. You pretend you are a customer of the pager company. You've been receiving other people's messages all day. In fact, you received one of this person's messages for Dr. [Name]. *Sound exasperated.* Ask the person for the number and pager ID that they called so you can clear it up with the pager company. *Thank them profusely.*

You can use the telephone number and pager ID to trigger a transmission over the air waves.

2. Grab the frequency. The resistance movement now has a telephone number and a pager ID that it can use to trigger the pager company into transmitting a message on a specific frequency. If you were to call from a public pay phone, you could *broadcast anonymously* over the air waves.

Step 3: Set up a broadcast schedule...

1. Distribute the frequency. The resistance movement informs each of its cells of the frequency. The leader sets up pre-arranged transmission times with his/her group of cells – for example, advise them to be monitoring the frequency at 7:45 pm each Tuesday.

2. Begin broadcasting. As an urban guerrilla, whenever you want to broadcast anonymously to your group of cells, you use a public pay phone to call the pager number and pager ID. Use pre-arranged coded messages that your cells will understand. For example, *"Let's change our appointment to Wednesday at 3"* might actually mean *"Switch to dead-letter box number 3"*.

Use coded messages that don't attract unwanted attention..

3. Anonymous reception. Provided that each of the cells *acquires a scanner* and is *tuned to the appropriate frequency* at the pre-arranged times, the entire group of cells will receive the broadcasts. There is no other contact between the leader and the cells. Security is watertight. Intelligence agencies and underground groups call this type of system a one-way radio link (OWRL).

When used properly, even the existence of the broadcast system will elude the authorities. The FBI can't eavesdrop on communications whose existence they're unaware of.

Step 4: Keeping the system secure...

1. Message content. Don't attract suspicion. The resistance movement leader uses innocuous messages that the legitimate pager user will simply dismiss as a *"wrong number"*.

2. Traffic volume. Don't attract unwanted attention. Don't overuse the system. The savvy urban guerrilla makes sure to intermingle this method with other methods. Use more than one pager ID and use more than one pager company.

3. Don't get traced. The savvy urban guerrilla never calls from a phone that can be associated with him/her. Today's digital telephony makes *instant* call-tracing a fact of life. Always initiate the broadcasts from a public pay phone. Use a different pay phone each time. Or use a phone borrowed at arm's-length (ie an office receptionist, a bar, a stranger's cell-phone, etc.).

Never call from a telephone that can be traced.

4. Adapt and innovate. Consider augmenting this system with other methods. A smart urban guerrilla will use the scanner to hack the system of a repair company that uses radio to keep in contact with its fleet of trucks. Consider phoning in to local radio *music-request lines* to broadcast to your cells. Use the *public-address system* of shopping malls, office buildings, etc. Some guerrilla groups hack into a third-party's answering service – once they've got their access code they can leave, pickup, and erase messages

anonymously. Use the telephone mailbox services of a singles' connection service.

NOTE – *Spy & CounterSpy* does not endorse, recommend, or suggest that you commit any illegal act. This article is provided for information, education, entertainment, and research purposes only.

SPY & COUNTERSPY

Spy school for the rest of us.

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com
EMAIL ENCRYPTION: Click on *Ask Agent X* for our public key.

How to use one-time pads for secret communications...

There is only one cipher system that cannot be cracked by the FBI or NSA – or by anyone else for that matter. That system is the *one-time pad*.

A message encrypted using a one-time pad cannot be broken because the encryption key is a *random number* and because the key is *used only once*.

A proven system. Intelligence agencies routinely use many different kinds of encryption systems – ranging from mechanical devices to invisible inks to computer software – but for *mission critical* messages that must be 100% secure they *always* use a one-time pad.

At the height of the cold war during the fifties and sixties, Soviet spies in the USA used one-time pads to communicate with their controllers, usually located inside Russian embassies and consulates. Not a single message was cracked by the FBI or NSA. And none of those messages ever will be cracked.

Used by the best. The one-time pad system is still being used today by intelligence agencies like Britain's MI.6, Germany's BND, France's DGSE, Russia's MBRF, and China's *Cheng Pao K'o*.

One-time pads are also being used by resistance groups like Northern Ireland's IRA, France's Action Direct, Uruguay's Tupamaros, Algeria's GIA, Lebanon's Hezbollah, Peru's Shining Path, and Argentina's Monteneros.

Inside this article. This article provides practical information that you can use to set up your own one-time pad encryption system. The article describes subtle refinements that you won't find in other books or articles. Our information comes direct from people with hands-on experience. Our two sources are an ex-MI.6 intelligence officer and a former member of Peru's Shining Path guerrillas. (Return to our home page and click on *About Us* for more on this.)

After studying this article you will have all the knowledge you need to set up a *100% secure system of communication* that cannot be cracked by the FBI, BATF, DEA, NSA, or any other organization.

If you're playing by Big Boys' Rules, the one-time pad will keep you out of the internment camps.

BACKGROUND – Cryptography as a science was originally developed by the Arabs. The year 1412 saw the publication of *Subh al-a 'sha*, a 14-volume encyclopedia written by Shihab al-Din al-Qalqashandi. The text described transposition and substitution ciphers. The Arabs were light-years ahead of the Europeans because their mathematics were more advanced – and cryptography relies heavily on math. While the Europeans were still struggling with Roman Numerals, the Arabs had already discovered the principle of zero.

The word cipher is derived from the Arab word *al cifr*, literally meaning nothing or zero.

The one-time pad system itself was perfected in 1917 during the first world war. Random keys were written on sheets of paper that were glued together to form a pad. Each key was used only once – hence the name, one-time pad.

Step 1: Create the key...

The core of the one-time pad system is the random key. A key is a block of numbers that is used to transform your original message (the plaintext) into a coded message (the ciphertext). Before you can begin to work with a one-time pad system, you need to create a random key. Before you can create a random key, you need a method for converting alphabet characters into numbers.

The chart below illustrates a workable system that is simple and easily remembered.

BACKGROUND – Government agencies use code-books containing often-used words and phrases that are represented by numbers. For example, rather than encrypting a phrase like *safe house 4* to 0916 2698 1402 2004 1301, the coding clerk might simply use 0219.

Spies and agents, on the other hand, cannot afford to carry incriminating evidence like bulky code-books, so they use instead the simplified conversion method shown below and spell out every word in full.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Now you're ready to create a key. First, write down a series of random alphabet characters, such as HLMSEZRBHPSJOTDW.

To make the key easier to work with, break it into blocks of

To make the key easier to work with, break it into blocks of two characters each, thus HL MS EZ RB HP SJ OT DW

Now use the conversion table shown above to convert the alphabet characters into numbers. For example H=08 and L=12, so the first block HL becomes 0812.

The result is 0812 1319 0526 1802 0816 1910 1520 0423.

You've just created your first *one-time pad*. This is also called the *key*. (Normally you would create a much longer key than this, enabling you to send a number of messages before the key is used up.) As you use the blocks of numbers to encrypt messages, you would cross out each block you've used. This will ensure that you use a block only once. (We'll simulate crossing out a block by graying it.)

0812 1319 0526 1802 0816 1910 1520 0423

You would normally create two copies of the key and provide one copy to your intended recipient.

Step 2: Format your message...

Suppose that the message you want to send is MY SECRET.

You would next format your message into blocks of two characters each, yielding MY SE CR ET.

Next, use the conversion chart above to convert the alphabet characters into numbers. In the example we're using M=13 and Y=25, so the first block would be 1325.

The entire string becomes 1325 1905 0318 0520. You can now see how using blocks makes the text increasingly difficult for anyone to crack, even at this stage.

Guidelines...

Use the character X to represent a period in your plaintext.

Rule 1 – Numbers. Spell out all numbers in full in your plaintext. For example, 365 becomes THREE SIX FIVE.

Rule 2 – Negatives. Always add emphasis to the word NOT in your plaintext. For example, you would write AGENT ALPHA NOT RPT NOT AVAILABLE FOR MEETING TUESDAY, where RPT stands for REPEAT.

Rule 3 – Punctuation. Use an X for each period in your plaintext. For example, MESSAGE RECEIVEDX SEND MORE INFOX. All other punctuation must be written out in full. For example, COMMA.

Rule 4 – Termination. End your plaintext with XX. If necessary, add dummy characters after XX in order to *pad out* the message to frustrate cryptanalysis and to conclude on a doublet (ensuring the numeric string ends with four digits).

Step 3: Encrypt your message...

We need some way to indicate to our recipient where the key begins, otherwise he/she won't be able to decrypt.

Remember in our earlier example, we created a key and stroked off (in gray) the blocks we'd already used. Here's what our key looked like.

0812 1319 0526 1802 0816 1910 1520 0423

The starting position in the key is at block 1319. So we'll place the string 1319 at the beginning of our message so the recipient will know how to decrypt. The plaintext message of 1325 1905 0318 0520 becomes 1319 1325 1905 0318 0529 because we place the pointer 1319 at the beginning of the string.

Use a pointer at the beginning of your message to specify the key so your recipient can decrypt the text.

We're now ready to encrypyt. First we write out the plaintext. Then directly below it we write out the key. Then we add the key to the plaintext using Fibonicci addition. This means we do no carrying. For example, 9 + 2 would yield 1 not 11. And 7 plus 6 would yield 3 not 13. Here's how the spy's working sheet would look.

Plaintext	1319	1325	1905	0318	0520
Key	--	0526	1802	0816	1910
Ciphertext	1319	1841	2707	0124	1430

The encrypted message 1319 1841 2707 0124 1430 is ready to be sent to our recipient. And we can sleep peacefully knowing that it cannot be cracked by anyone except the recipient.

Decrypting the message...

To decrypt a message, we simply reverse the calculations. We subtract the key from the ciphertext using Fibonicci subtraction. This means we allow no negative numbers. We add 10 if required. For example, 2 - 9 would yield 3 (because we add 10 so that we're able to subtract 9 from 12).

The first block in the ciphertext tells our recipient where to start in the key.

Here's what the recipient's working sheet looks like.

To decrypt the message, the recipient simply reverses the calculations.

Ciphertext	1319	1841	2707	0124	1430
Key	1319	0526	1802	0816	1910
Plaintext	--	1325	1905	0318	0520

Here's how we subtract 0526 from 1841.

The first column is 1 - 0 = 1.

The second column is 8 - 5 = 3.

The third column is 4 - 2 = 2.

The fourth column is 1 - 6 = 5 (because 11 - 6 = 5).

Using the conversion chart described earlier, the recipient converts the string of numbers back into alphabet characters. In this example, 13=M and 25=Y, so the first block 1325 converts to MY. The string 1325 1905 0318 0520 becomes MY SE CR ET.

The recipient reformats it to become MY SECRET.

About security...

Provided that an eavesdropper cannot get access to either the sender's or receiver's key, the one-time pad method is 100% secure. No FBI *cryptanalyst* will ever crack it. No Cray supercomputer running the NSA's *cracker software* will ever break it. Period.

But you need to be prudent about security.

Key security. Good security means you must conceal your key in a location where you'll know if it's been tampered with. Usually this means carrying it on your person *at all times*.

Location security. Good security means choosing private locations to encrypt and decrypt your messages. Remember, it's easy for FBI agents or local police to install a pinhole video camera above your desk. When choosing a location, be creative, be unpredictable, and be quick.

SURVIVAL TIP – At the first sign of surveillance you must stop working at your desk unless you're absolutely sure there's no way they can gain access to install the video surveillance equipment. In a pinch you can work *under* your desk until you implement off-site locations.

Disposal security. Good security means destroying your working materials after each encryption or decryption. Don't leave anything around for the authorities to work with. This usually means shredding and burning – or ingestion. (Yes, *eat* the evidence. It saved Kim Philby's bacon early in his career.)

Random means just that. The security of your one-time pad system depends on the randomness of the key. Don't use a computer to generate your keys. Do it by hand – and be sure to introduce a second element of randomness into your method by throwing dice or flipping a coin every now and then while you're creating your keys.

One-time means just that. Don't use a key more than once. Ever. Even if just a few blocks overlap in two different messages, the NSA cracker software will shift and compare the ciphertext messages until the statistical frequency of characters matches the expected statistics for English language text. Giving the NSA an opening like this is tantamount to setting the fox loose in the hen-house.

The perfect system. When used correctly, the one-time pad system provides perfect security for your secret messages. The weakest link is the human element.

How to test your skills...

Here is a piece of ciphertext and a one-time pad you can use to verify your new skills.

The first four-digit

group is a pointer to the starting place in the one-time pad.

The one-time pad is 0916 0305 2521 2113 0119 0605 1413 2024 0806 0518 1306 0602 1710 2022 0410 0804 2301 2116 1512.

The ciphertext is 0119 2110 3521 2739 2026 0113 1414 1527 2231.

Remember that the first four-digit group in the ciphertext is a pointer indicating where to begin in the one-time pad.

SPY & COUNTERSPY

Spy school for the rest of us.

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com

How to evaluate new members...

Weed out informants and agent-provocateurs.

Assessing the risks. It is imperative that you run tests to verify the reliability and integrity of new recuits who are applying to join your cell. Failure to evaluate recruits will result in your group being penetrated by your adversary – much like the militia groups in the USA have been penetrated by the FBI.

Every time you admit a new recuit into your cell you are risking the security of your group. Yes, the recruit might be a *bona fide* supporter of your cause – or he might be an informant or an agent-provocateur.

The Informant. The informant is a cell member who is providing information to your adversary. He may betray you for money. She may betray you because she is being blackmailed. He may betray you because he is unethical, immoral, and weak-willed. She may betray you because she has a passive-aggressive personality disorder.

The Agent-provocateur. The agent-provocateur is someone who feigns enthusiastic support for your cause while enticing you to commit acts that are illegal. She is acting on the instructions of the FBI – or she may actually be an FBI agent. You are being set up for arrest, interrogation, and conviction.

The Mole. The mole is a cell member who quietly works to sabotage your operations. He may deliberately *forget* to do things that result in failed operations. He may intentionally *ruin* meetings with specious arguments and pointless debate, often introducing paranoia into the discussion. A typical mole is a long-time cell member who has been recruited by the FBI, perhaps by blackmail. Less frequently the mole is an FBI agent who has penetrated the organization at an early stage in its development.

The Counterintelligence Role. It is vital that your organization have a *counterintelligence officer*. This is someone whose role is to detect and neutralize attempted penetrations by the enemies of your organization. Whether this is a formal position or an *ad hoc* role is not important. Someone in your group must take steps to systematically and conscientiously evaluate new recuits.

If you don't make an effort to defend yourself against penetration by your adversary, then you'll end up like the militia groups in the US... paranoid, disorganized, ineffective, and – more often than not – in custody.

Uncover informants...

Here is how established resistance movements uncover informants.

First, reveal some sensitive information to the recruit – and *only* to the recruit. For example, you might inform him of the existence of a (bogus) hidden cache of weapons.

Reveal some sensitive bogus information to the suspected informant, then wait for things to go wrong.

Then wait and watch. If the cache is suddenly discovered by the authorities, you may be dealing with an informant. More tests may be required to confirm your suspicions.

In serious cases where you're playing by Big Boys' Rules, you might need to use live bait. If your adversary is sophisticated and experienced, you might need to reveal genuine secrets to the recruit you're evaluating. For example, you might reveal the name of a *whistleblower* who is leaking information to you about your adversary. If your recruit betrays your information to your adversary, you'll have lost your whistleblower – but you'll have unmasked an informant before he can do too much damage.

Unmask an agent-provocateur...

Here is how any organization can unmask an agent

Here is how any organization can unmask an agent-provocateur.

The most reliable method for unmasking an agent-provocateur is to ask him to be the first to commit to action.

If the person is full of ideas for future operations, then *insist that he lead by example*. Make him commit himself first. Or, to put it another way, make him incriminate *himself* first before asking others to risk injury, exposure, or arrest.

If the person balks, then he may simply be "all talk". Or he may be a coward. Or he may be an agent-provocateur. In either case, you've called his bluff and now you know not to fall for his *jive-talk*.

Enforce compliance...

Here is how resistance movements enforce compliance with the counterintelligence functions.

If a trusted cell member brings an outsider into your group – or reveals sensitive information to an outsider – without performing any of these counterintelligence measures, then that cell member must be severely disciplined.

Depending on your situation, simply ostracizing the individual may suffice. Revoking his membership may be all it takes to remove the threat he poses. Or firmer steps may need to be taken.

SPY & COUNTERSPY

Spy school for the rest of us.

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com
EMAIL ENCRYPTION: Click on *Ask Agent X* for our public key.

A primer for whistleblowers – How to send anonymous email...

Imagine, for a moment, this hypothetical situation. You possess inside information. You feel the public has a right to know. You are a moral individual and you have a strong sense of social responsibility. But you don't want the goons kicking in your door an hour before dawn. Your problem is – you don't know how to leak the information *without getting caught*. You don't know how to communicate anonymously.

What you'll learn here...

This article teaches you how to use the Internet to send untraceable email. The recipient of the message won't be able to trace you. The Internet provider won't be able to trace you. The local phone company won't be able to trace you. The FBI won't be able to trace you.

Simply stated, if you need tradecraft that will give you *unbreakable* anonymity, you are reading the right article.

Step 1: Get online anonymously...

First, go to a cybercafe. This is a retail store that offers public access to the Internet. You'll find them in almost every US city.

The cybercafe you select should ideally be in another city. At a minimum, it should be on the other side of town. Don't use the cybercafe just around the corner from where you work.

Some cybercafes charge by the hour, others by the minute. Some are free, located in public libraries and colleges. But otherwise they all work the same way. You sit down at a computer workstation and use it as if it were your own.

It's already preloaded with nifty software, including the most popular browsers. And it's connected to the Internet. You can surf the 'net just like you do at your office or home. Except when you're using a cybercafe you're anonymous.

BACKGROUND – You can't use your own computer and expect anonymity. The authorities can trace email packets back to your SMTP and POP accounts at your Internet service provider. From there the telephone line or coaxial cable can be traced to your physical location.

With today's digital infrastructure, the trace is instantaneous. There's no hurry, though. Billing records allow the authorities to trace you months later if need be. So-called *remailers*, *anonymizers*, and *mixmasters* are helpful, of course – they'll slow down the authorities' search by about 24 hours – that's about how long as it takes to serve a warrant or writ on an uncooperative Webmaster.

Protect your identity...

Whether you pay the cybercafe proprietor in advance or afterwards is not important. But you must make a point to pay using cash. And don't show any ID. If the proprietor insists on credit card payment or personal ID, go elsewhere.

When trained members of a resistance movement use cybercafes, they alter their *silhouette* by wearing different clothing and footwear, changing their hairstyle, adding (or deleting) eyeglasses, and so on. Simply wearing a hat can significantly reduce the ability of a witness to describe your appearance to an investigator. It can also confound an in-store video surveillance camera.

Step 2: Set up an email account...

As soon as you are online at the cybercafe, you can set up an anonymous free email account. Here are a few providers to choose from – mailexcite.com, prontomail.com, usa.net, hotmail.com, mailcity.com, and doghouse.com.

Other providers are available. Use a search engine to find one that meets your preferences.

Getting registered...

As you complete the online registration form, keep in mind that

the provider has no way of verifying the information you provide. For all he knows, you might be using a fictitious name, address, postal code, and telephone number. Not all providers even bother to request this information. Some ask for only a name and a city.

Remember that the name you provide will appear on the header of outgoing email messages.

If the registration form insists on an email forwarding address or a social security number, you should look elsewhere for a provider.

After submitting the registration form, you'll usually have an active email account within a few moments. You can now send and receive email anonymously.

Intelligence agencies refer to this type of arrangement as a *cover address*.

Intelligence agencies refer to this type of arrangement as a *cover address*. In particular, a cover address refers to a postal address, email address, or courier address that is not linked to the identity of the person using the address.

Step 3: Send your message...

If you have a short message to transmit, simply type it into the editing window of the email editor and you can send your email immediately.

If you have a longer message...

If you have a lengthy message or an encrypted message to transmit, you should prepare it in advance and bring it with you on diskette as a text file or html file. Most cybercafes allow you to use diskettes with their computers. Simply insert the diskette as you would at your office or at home.

SECURITY CAUTION – If your cybercafe insists on inserting the disk at a central location and then transmitting the data by LAN (local area network) to your computer workstation, you'll probably want to use encrypted text. Some cybercafes do this because they're concerned about viruses being introduced into their systems.

You can use Windows Wordpad to load your file, select the text, and copy it to the Windows clipboard. Then you'll be able to use Shift+Ins to paste your text into the editing window of the email editor.

You can also send your file as an email attachment direct from your diskette. Different email account providers have different policies concerning attachments. Some allow them. Some don't.

Limiting your exposure...

Under most circumstances, you'll be able to get online, set up an anonmous free email account, compose and send your message, and log off in fewer than 3 minutes. There's no real need to rush, however. You don't want to attract attention to yourself.

Step 4: Cover your tracks...

Take a damp cloth. Wipe off the keyboard. Wipe off the mouse. Wipe off anything else you've touched. Don't leave any fingerprints.

Make certain you've removed your diskette from the disk drive. If you have a DOS-based file-wipe utility, you can use it to delete the browser's cache files, history files, and bookmark file. (This step does nothing to hinder the authorities, however, who can trace the source of the email message to this particular computer if they open an investigation. Deleting the browser's files merely obstructs nosy busybodies – other cybercafe customers and staff.)

Go to the counter and pay the proprietor. With cash.

Wipe the keyboard.
Remove your diskette.
Pay the cybercafe.
Walk out the door.
And don't go back.

Disappear forever...

Walk out the door. Don't go back. Ever. And keep your secret to yourself. Don't tell anyone. Ever.

BACKGROUND – Keeping quiet is important. Most people are caught because they can't resist the urge to brag – or because they feel a need to confide in someone. If you can't keep a secret, then you'll never be a good underground urban activist, freedom fighter, or guerrilla.

Intelligence agencies, security services, resistance movements, and guerrilla groups have found that for some reason women seem better at keeping quiet about covert ops than men. So if you're a guy, you'll need to make an extra effort in this regard.

Smile to yourself. Congratulations are in order. You've just executed a successful covert op. **;)**

Spy school for the rest of us.

Back to Home Page

Here is the small print. It appears here because we have found that maintaining a corporate front is the only way we can protect ourselves against interference by governments and their agencies. The legal underpinnings of our corporate front are our first line of defense against audit-attacks and other methods of economic warfare that the authorities use to suppress dissent, protest, and activism. They are also determined to prove their hypothesis that *Spy & CounterSpy* is funded by a foreign intelligence agency or terrorist group – but our double entry accounting record of corporate revenue and expenses is our shield against fabricated evidence by an overzealous investigator or case officer.

Lee Adams Seminars is a division of Here's-how, Right-now! Seminars Inc.
OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com

Tax resistance primer – How to beat the IRS...

WARNING – Tax evasion is a criminal offense. Don't do it. The material in this article is presented for information, research, entertainment, & education purposes only.

You probably don't realize that *big government* sticks its hand in*your pocket* and takes *half* of everything it finds there. Every time money change hands, government bureaucrats skim their cut off the top.

A growing doubt. Across America, more and more citizens are losing confidence in their government. Common, decent folk are losing faith – they look around them and see unresponsive elected officials, national ID cards, gun registration, militarized police, property confiscation, rampant surveillance, a cashless society, a tethered news media. They remember Vickie Weaver. They remember Waco.

Decent Americans are beginning to see the effects of *no-knock* warrants, coerced informants, illegal arrests, rigged trials.

At the international level, more and more Americans are troubled by a foreign policy indistinguishable from terrorism – and a disgraced (but still arrogant) national leadership.

The list goes on and on.

These hard-working, decent Americans no longer believe their government represents them. These citizens no longer accept that the government has any moral right to take their hard-earned money.

These patriotic, otherwise law-abiding citizens are rallying to the same cry that stirred the heroes and heroines of the American Revolution – *no taxation without representation*.

How the world really works. Stop for a moment and consider this scenario. If you earn a hundred dollars the government grabs 35% as income tax. That leaves you with $65.00 in your pocket. If you wanted to buy $100.00 worth of groceries you'd actually need to earn $155.00 just to have $100.00 left in your pocket.

But it doesn't stop there. When you go to pay for your $100.00 groceries, the seller tacks on the sales tax. Between state tax, county tax, local tax, hidden manufacturing taxes, licensing fees, permits, excise, duty, etc. etc. etc. in many cases the sales tax exceeds 15%. So now you're paying $115.00 for $100.00 worth of groceries. To get that $115.00 you need to earn $180.00.

NOTE – In all fairness, we're playing loose and fast with figures here in order to get our point across. Other taxes, rebates, exemptions, licensing fees, permits, and surcharges apply, but they only serve to complicate the issue – these factors don't alter the fundamentals of the racket being foisted on us by the gangsters... err, we mean the *government*.

What you'll learn here...

This article teaches you a method of tax resistance that allows both parties in a transaction to *keep every dollar* they earn.

This system is already being successfully used in the USA by individuals and small businesses. The IRS doesn't want you to know about this method because they *don't know how to stop it*. Simply stated, this article shows you how to beat the IRS.

IMPORTANT NOTE – *Spy & CounterSpy* does not condone any illegal act. Tax evasion is a crime. Don't do it. You shouldn't let your judgment be clouded by the fact that IRS "inspection agents" routinely carry concealed handguns in direct violation of federal and state law. Just because the IRS routinely breaks the law doesn't mean you should too. Remember, the material in this article is presented for information, research, entertainment, and education purposes only.

Lesson 1: How to guarantee you'll continue to be fleeced by the government...

Let's consider a simple deal in which I agree to buy an item from you for $100.00.

Sales tax. You must collect the sales tax from me. Let's assume it's 15% (federal, state, county, and local all added together). That means I actually pay $115.00 (not $100.00) for the $100.00 item I've agreed to buy from you. Government gets the $15.00. As the buyer, I pay the sales tax under threat of imprisonment.

imprisonment.

Forced labor. You as the seller, meanwhile, are forced to do the government's paperwork – you must *calculate* the tax, *collect* it from me, and *remit* it to the government. You as the seller do all this work for *free*, again under threat of imprisonment.

Income tax. You, as the seller, receive $100.00 for the item. Let's assume your wholesale cost is $50.00. That means your real earnings are $50.00 (for your labor, etc.). Let's assume an income tax rate of 30% (it's often higher). When you fill out your income tax form next spring you're going to find that you must pay the government $15.00 on the $50.00 you earned. So you as the seller really make only $35.00 on a $100.00 transaction. As the seller, you pay your income tax under threat of imprisonment.

The bottom line. In the simple example given here, the government skimmed $30.00 off a $100.00 transaction. They took $15.00 from me, the buyer. They took another $15.00 from you, the seller.

In actual practise, however, the government takes *a lot more* than this. We haven't considered the wholesaler or the manufacturer, who will each be paying 30% income tax on their revenue too. Nor have we considered that the buyer needs to earn $155.00 in order to have $100.00 in his/her pocket. If all parties are considered, the government skims more than 50% off *each and every transaction* every day in America. All under threat of imprisonment, of course.

Four hundred years ago we had a name for people who did things like this. We called them *robber barons*.

NOTE – Government bureaucrats need an efficient money-raising system like this if they're going to keep buying $600.00 hammers and $400.00 screwdrivers for their departments. If you ever need a good laugh, consider looking through the auditors' reports on how these idiots waste our tax dollars. They often spend money *just for the sake of spending it* – in order to ensure their department gets a bigger budget next fiscal year. It's insanity, but that's business-as-usual for the government.

Lesson 2:
How to *pretend* you're not being fleeced by the government...

WARNING – Tax evasion is a criminal offense. Don't do it. The material in this article is presented for information, research, entertainment, & education purposes only.

Let's assume you agree to have some electrical work done in your office for $100.00.

Suppose the electrician is a tax resister. He might wink at you and say, "If you'll pay me cash, I won't charge you any sales tax."

(No nasty email please. We've got nothing against electricians, most of whom are good people.)

You, being somewhat of a rube at the tax resister game, agree to this conspiracy. After all, you figure you're saving the 15% sales tax. And you don't need a receipt.

Unfortunately, however, things aren't that simple. One of you is still getting fleeced.

The buyer's dilemma. If you're in business, you can't claim what you spent as an expense – because you didn't get a receipt. So you're still stuck in the position of needing to earn $155.00 in order to be able to spend $100.00. Of course, these calculations are hidden and the stark reality doesn't really confront you until next spring when you're filling out your income tax forms.

The seller's situation. The electrician did okay. Because he issued no receipt to you, there is no record of the cash transaction. So he might be tempted not to declare the money as revenue. In that case the seller pays no income tax. So he gets to keep the full $50.00 he earned ($100 minus his wholesales costs of $50.00).

The seller is a happy camper. But once you figure out what's happened to you, you're unlikely to fall for the *no-sales-tax* ploy a second time. That's because the seller is beating the IRS, but it's at the buyer's expense. In other words, he beat the IRS but you didn't.

You're probably asking yourself, "Gee, there must be a better way, where both buyer and seller come out ahead of the IRS."

And there is.

Lesson 3:
How to beat the tax man...

The key to a successful, audit-proof, tax resistance strategy is the *receipt*.

Pay attention. Here's how tax resisters across America beat the

WARNING – Tax evasion is a criminal offense. Don't do it. The material in this article is presented for information, research, entertainment, & education purposes only.

IRS every day.

The seller winks and says, "If you'll pay me in cash, Mr. Buyer, I won't charge you the sales tax."

The buyer replies, "Sure, I'd be glad to, but I'll still need a receipt for income tax purposes."

"Of course," says the seller, who proceeds to make out a receipt for the buyer *under the name of a non-existent firm*.

Both parties win. Here's why...

The buyer is happy. The buyer saves 15% off the top. He doesn't pay any sales tax on the transaction. Plus, he gets to claim his purchase as a legitimate expense because he's got a receipt to staple to his tax form next spring. So he only needs to earn $100.00 in order to be able to spend $100.00.

The seller is happy. The seller saves 30% income tax on his earnings. It's a cash transaction so there's no record of the sale. So he doesn't declare the income. The preprinted receipt he gave the buyer is under the name of a non-existent company that cannot be traced to the seller.

Criminal conspiracy. Let's be frank. What we're describing in this article is criminal conspiracy and collusion. The IRS has found that, if both parties keep quiet about what they've done, this method of tax resistance is *audit-proof*, provided that the method isn't flagrantly overused.

SECURITY NOTICE – The "inspection agents" of the IRS will, however, open your mail, bug your home or office, and put you under surveillance in their attempts to get you. Whistleblowers at the IRS have told *Spy & CounterSpy* that these goons carry guns – in direct violation of federal and state law, of course.

Thousands of transactions are conducted across America every day using this method of tax resistance. Yes, it's illegal. Yes, it's criminal fraud. Yes, it's tax evasion. Don't do it. Simply put, it would be unlawful for *Spy & CounterSpy* to encourage you to join the thousands of Americans who already practise tax resistance because they have lost faith in their government.

Summary. The *receipt* is what makes this method of tax resistance successful. The IRS doesn't want you to know about it because they don't know how to stop it.

NOTE – *Spy & CounterSpy* does not endorse, condone, or encourage any illegal act. Tax evasion is a criminal offense. Don't do it. The material in this article is presented for information, research, entertainment, and education purposes only. The words "you" and "your" are used in this article for ease of readability only.

For other tax resistance and tax reduction strategies, interested readers may find the information at http://www.taxgate.com useful. (This is an external link unrelated to Spy & CounterSpy.)

SPY & COUNTERSPY

Spy school for the rest of us.

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com

Surveillance team communication codes...

Members of a surveillance team use code-words to communicate with each other. This reduces the possibility of an eavesdropper discovering the existence of the surveillance team.

The code-words described here were leaked to us in mid-1997 by one of our sources inside a US government agency. They are used mainly with the *floating-box* method of surveillance. Both *wheel artists* and *pavement artists* use code-words for transmitting to other team members during a surveillance operation.

NOTE – This is only a partial listing of code-words used in surveillance operations. A surveillance team that specializes in following targets during their commute to and from work will use code-words that are different from those used by a surveillance team that is following drug traffikers on foot in the downtown core.

Part One: The code-words...

The plaintext appears first, followed by the ciphertext code-word.

AIRCRAFT – bee
AIRPORT – hive
ANTISURVEILLANCE – smoke, fog
BANK – wallet
BAR – lair
BRIDGE – lizard
BRUSH PASS – bolt
BUS – beetle
CAMERA – cheese
CHURCH – star
CITY – domain
COMMAND OF THE TARGET – zero zero, alive
CONSTRUCTION – turtle
CONTACT – strike
COUNTERSURVEILLANCE – fire
DEAD DROP – ash
DIRECTION OF TRAVEL – facing
DISGUISE – suntan, tanned
DOWNTOWN – empire
ELEVATOR – rocket
ENTER, GO INSIDE – infect
ENTRANCE DOOR – snare
EXIT, LEAVE, DEPART – cure
FEMALE – socket
FILL UP VEHICLE – sip
FREEWAY – python
GAS STATION – feeder
HIGHWAY – python
HIGHWAY RAMP, INTERCHANGE – viper
HOSPITAL – cross
HOTEL, MOTEL – cage
HOUSE – trap
INTERSECTION – cobra
LEFT LANE – inside
LIGHT, ILLUMINATION – sword
MALE – plug
MEETING – strike
ON FOOT – free
PARKING LOT – corral
PEDESTRIAN – rat, hamster, gerbil
POLICE – stick, cuffs
POST OFFICE – pen
PUBLIC PARK – farm
RENDEZVOUS – knot
RESTAURANT – roost
REST ROOM – bowl, bowl patrol
RIGHT LANE – outside
SCHOOL – zoo
SPEED OF TRAVEL – pedal
STOPPED – dead, comatose
STORE, SHOP – cave

STREET – snake
SUBWAY – worm
SURVEILLANCE DETECTION – spark
TARGET – beta
TARGET'S VEHICLE – gamma
TARGET'S RESIDENCE – omega
TARGET'S WORKPLACE – epsilon
TAXI – termite
TELEPHONE – carrier pigeon
TEMPORARILY STOPPED – snagged, daydreaming
TERMINATE SURVEILLANCE – crash
TRUCK (COMMERCIAL) – slug
TRUCK (PICKUP, VAN, 4x4) – bug
U-TURN – flip

Part Two: Sample messages...

Sample #1:
TARGET VEHICLE IS STOPPED AT RED LIGHT.
Gamma is daydreaming at the sword.
Sample #2:
TARGET HAS JUST ENTERED A BAR.
Beta rat has infected the lair.
Sample #3:
TARGET VEHICLE IS TRAVELING IN THE LEFT LANE AT 30 MPH AND IS THE THIRD VEHICLE AHEAD OF A BLUE PICKUP TRUCK.
Gamma is inside at pedal three zero, three up on the blue bug.
Sample #4:
TARGET VEHICLE HAS JUST MADE A U-TURN. MIGHT HAVE DETECTED US.
Gamma is flipping, possible spark or smoke.
Sample #5:
LIGHTS HAVE JUST GONE OUT AT TARGET'S RESIDENCE. TERMINATE SURVEILLANCE FOR TODAY.
The omega swords are off. Crash.

NOTE – Occasionally an agent makes a mistake and transmits a message in the clear. However, agents are trained not to repeat the message using code-words, because doing so would give an eavesdropper both the plaintext and the ciphertext.

SPY & COUNTERSPY

Spy school for the rest of us.

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com
EMAIL ENCRYPTION: Click on *Ask Agent X* for our public key.

Updated October 28th, 1998. Errors or omissions will be corrected if brought to our attention.

Spy address book...

SUBMISSIONS – *Spy & CounterSpy* welcomes email containing the address and telephone number of intelligence agencies and security services.

USA...

CIA – Washington DC 20505. Telephone 703.482.1000. Fax 703.482.6790.

CIA Paris station – Tel. 4296.12022 extension 2306.
CIA London station – Tel. 499.9000 extension 2394.
CIA Rome station – Tel. 46741 extension 2694.

NSA – Fort George G. Meade, Maryland 20755 6000. Telephone 301.688.6311.

BATF – Suite 4100, 650 Massachusetts Ave., Washington DC 20226.

DIA – Boling Air Force Base, Washington DC 20340. Telephone 703.695.0071.

FBI – Suite 7110, 935 Pennsylavania Ave. NW, Washington DC 20535 001. Telephone 202.324.4880. Fax 202.324.4228.

FBI field offices

11000 Wilshire Boulevard, Los Angeles CA 90024, Tel. 213.477.6565.
1142 Ambassador Road, Baltimore MD 21207, Tel. 301.265.8080.
200 West Orace Street, Richmond VA 23220, Tel. 804.644.2631.
115 Federal Building, Butte MT 59702, Tel. 406.782.2304.
16320 2nd Ave. NW, Miami FL 33169, Tel. 305.944.9101.
26 Federal Plaza, New York NY 10278, Tel. 212.553.2700.
2704 Federal Building, St. Louis MI 63103, Tel. 314.241.5357.
10th floor, 275 Peachtree Street NE, Atlanta GA 30302, Tel. 404.521.3900.
3005 Federal Office Building, Cleveland OH 44199, Tel. 216.522.1400.
3203 Federal Building, Salt Lake City UT 84138, Tel. 801.355.7521.
392 Federal Building, Minneapolis MN 55401, Tel. 612.339.7861.
450 Golden Gate Avenue, San Francisco CA 94102, Tel. 415.553.7400.
535 West Jefferson Street, Springfield IL 62702, Tel. 217.522.9675.
5401 Paulsen Street, Savannah GA 31405, Tel. 912.354.9911.
01 Grand Avenue NE, Albuquerque NM 87102, Tel. 505.247.1555.
5th floor, 445 Broadway, Albany NY 12202-1219, Tel. 518.465.7551.
6010 Kenley Lane, Charlotte NC 28217, Tel. 704.529.1030.
6015 Federal Building, Houston TX 77002, Tel. 713.224.1511.
700 E. Charleston Boulevard, Las Vegas NV 89104, Tel. 702.385.1281.
841 Clifford Davis Federal Building, Memphis TN 38103, Tel. 901.525.7373.
8th floor, 600 Arch Street, Philadelphia PA 19106-1611, Tel. 215.829.2700.
Crown Plaza Building, Portland OR 97201, Tel. 503.224.4181.
Room E222, 701 C Street, Anchorage AK 99513, Tel. 907.276.4441.
Federal Building, New Haven CT 06510, Tel. 203.777.6311.
Federal Building, Sacramento CA 95925, Tel. 916.481.9110.
John F. Kennedy Federal Office Bldg., Boston MA 02203, Tel. 617.742.5533.
4th floor, 7820 Arlington Expressway, Jacksonville FL 32211, Tel. 904.721.1211.
One St. Louis Centre, Mobile AL 36602, Tel. 205.438.3674.
477 Michigan Avenue, Detroit MI 48226, Tel. 313.965.2323.
Room 526, Federal Building, San Juan PR 00918, Tel. 809.754.6000.
Room 679, 575 N. Pennsylvania St., Indianapolis IN 46204, Tel. 317.639.3301.
Room 700, Federal Building, Milwaukee WI 53202, Tel. 414.276.4684.
Room 710, 915 Second Avenue, Seattle WA 99174, Tel. 206.622.0460.
Room 1300, Federal Office Building, Pittsburgh PA 15222, Tel. 412.471.2000.
Room 1823, Federal Office Building, Denver CO 80202, Tel. 303.629.7171.
Room 300, US Court House, Kansas City MO 64106, Tel. 816.221.6100.
Room 4307, Kalanianaole Federal Building, Honolulu HI 96850, Tel. 808.521.1411.
Room 433, 615 E. Houston, San Antonio TX 78205, Tel. 512.225.6741.
Room 500, 300 N. Lee Street, Alexandria VA 22314, Tel. 703.683.2680.
Room 502, 600 Federal Place, Louisville KY 40202, Tel. 502.583.3941.
Room 610, Federal Office Building, Tampa FL 33602, Tel. 813.228.7661.
Room 6S-31, 880 Front Street, San Diego CA 92188, Tel. 619.231.1122.
Room 7401, Federal Building, Omaha NE 68201, Tel. 402.348.1210.
Room 800, 1111 Northshore Drive, Knoxville TN 37919, Tel. 615.588.8571.
Room 839, 200 Granby Street, Norfolk VA 23510, Tel. 804.623.3111.
Room 90, Everett M. Dirksen Bldg., Chicago IL 60604, Tel. 312.431.1333.
Room 9023, 550 Main Street, Cincinnati OH 45202, Tel. 513.421.4110.
Suite 200, 10825 Financial Centre Parkway, Little Rock AR 72201, Tel. 501.221.9100.
Suite 2200, 1250 Poydras Street, New Orleans LA 70113, Tel. 504.522.4671.
Suite 300, 180 North Lamar Street, Dallas TX 75202, Tel. 214.720.2200.
Suite 400, 201 East Indianola, Phoenix AZ 85012, Tel. 602.219.5511.
Suite C-600, 700 E. San Antonio Ave., El Paso TX 79901, Tel. 915.533.7451.
Suite 1357, 18 S. Assembly Street, Columbia SC 29201, Tel. 803.254.3011.
Suite 1600, 50 Penn Place, Oklahoma City OK 73118, Tel. 405.842.7471.

US Secret Service field offices

Frederick MD, Tel. 301.293.1958.
Fresno CA, Tel. 209.487.5204

Grand Rapids MI, Tel. 616.456.2276.
Great Falls MO, Tel. 406.452.8515.
Greenville SC, Tel. 803.233.1490.
Harlington TX, Tel. 512.428.9311.
Harrisburg VA, Tel. 717.782.4811.
Honolulu HI, Tel. 808.541.1912.
Houston TX, Tel. 713.229.2755.
Jackson MS, Tel. 601.965.4436.
Jacksonville FL, Tel. 904.724.4530.
Kansas City KA, Tel. 816.426.5022.
Knoxville TN, Tel. 615.673.4527.
Las Vegas NV, Tel. 702.388.6446.
Lexington KT, Tel. 606.233.2453.
Little Rock AR, Tel. 501.378.6241.
Los Angeles CA, Tel. 213.894.4830.
Louisville KT, Tel. 502.582.5171.
Lubbock TX, Tel. 806.743.7347.
Madison WI, Tel. 608.264.5191.
Melville NY, Tel. 516.249.0404.
Memphis TN, Tel. 901.521.3568.
Miami FL, Tel. 305.591.3660.
Midland TX, Tel. 915.683.6923.
Milwaukee WI, Tel. 414.291.3587.
Minneapolis MI, Tel. 612.348.1800.
Mobile AL, Tel. 205.690.2951.
Montgomery AL, Tel. 205.832.7601.
Nashville TN, Tel. 615.251.5841.
New Haven CN, Tel. 203.865.2449.
New Orleans LA, Tel. 504.589.4041.
New York NY, Tel. 212.466.4400 extension 2184
Newark NJ, Tel. 201.645.2334.
Norfolk VA, Tel. 804.441.3200.
Oklahoma City OK, Tel. 405.231.4476.
Omaha NB, Tel. 402.221.4671.
Orlando FL, Tel. 305.648.6333.
Oxford MS, Tel. 601.236.1563.
Panama City FL, Tel. 904.265.5323.
Philadelphia OH, Tel. 215.597.0600.
Phoenix AZ, Tel. 602.261.3556.
Pittsburgh PA, Tel. 412.644.3384.
Portland OR, Tel. 503.221.2162.
Providence RI, Tel. 401.331.6456.
Raleigh NC, Tel. 919.790.2834.
Reno NV, Tel. 702.784.5354.
Richmond VA, Tel. 804.771.2274.
Riverside CA, Tel. 714.351.6781.
Roanoke VA, Tel. 703.982.6208.
Rochester NY, Tel. 716.263.6830.
Saginaw MI, Tel. 313.234.7223.
Salt Lake City UT, Tel. 801.524.5910.
San Antonio TX, Tel. 512.229.6175.
San Diego CA, Tel. 619.557.5640.
San Francisco CA, Tel. 415.556.6800.
San Jose CA, Tel. 408.291.7233.
San Juan PR, Tel. 809.753.4539.

Britain...

SIS (MI.6) – Century House, Vauxhall Cross, London.
SS (MI.5) – Thames House, Millbank, London.

Russia...

GRU – 11 Znamenka Street, Moscow. Telephone 095.296.03.65.
SVR – Yasenevo 11 Kolpachny, Moscow 10100. Telephone 095.923.62.13.
FCS – Lubiank 2, Moscow.
MBRF – unknown.

Germany...

BND – Bonn, 82 - 042 Pullach, Postfach 120. Telephone 089.793.0190.
BfV – Merianstrasse 100, W-5000 Koln 71. Telephone 0221.7920.

France...

DST – 7 rue Nelaton, Paris 75015. Telephone 45.71.49.42.
DGSE – 141 Boulevard Mortier, Paris 75020. Telephone

40.65.30.11.
RG – unknown.

Israel...

Mossad – unknown.
Shin Beth (GSS) – unknown.

Canada...

CSIS – PO Box 9732 Station T, Ottawa, Ontario, K1G 4G4, Canada. Telephone 613.993.9620.

Iraq...

Al Amn Al-Khas – unknown.
Da' Irat al Mukhabarat al-Amah – unknown.
SAVAK – unknown.

Australia...

ASIO – GPO Box 2176, Canberra, ACT, 2601. Telephone 02.6249.6299. Fax 02.6257.4501.
ASIS – unknown.

China...

Cheng Pao K'o – unknown.
Guoanbu – unknown.
ILD – unknown.

Japan...

Chobetsu – unknown.
Jetro – unknown.
Koancho – unknown.
MITI – unknown.

Iran...

QODS – unknown.

SPY & COUNTERSPY

Spy school for the rest of us.

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.

FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com

SPY & COUNTERSPY

Providing knowledge and skills to supporters of freedom and fairness.

Action Training

Proven methods for recognizing and thwarting FBI surveillance

Beating the FBI

At best, the FBI does not have a history of respect for civil rights. Whether you are guilty or innocent doesn't matter. You are always treated the same way during an FBI investigation – unfairly. Especially if surveillance is involved.

If you snooze, you lose. It's that simple. Many of us are sleepwalking through life. And if you don't pay attention, then you're gonna pay – especially if you engage in behavior that attracts the attention of the FBI.

Make no mistake about it, FBI surveillance teams are lethal. They are very effective at what they do. They have had lots of experience. They've got massive resources. In a major investigation, 30 agents watching one person is commonplace. You never see the same agent twice. You never see the same vehicle twice.

The FBI's triple-threat surveillance strategy of *multi-layered teams*, *rapid response*, and *managed aggression* must be taken seriously.

Threat #1 – A multi-layered team can fool you into thinking that the surveillance has ended. This is an extremely dangerous situation. They're still lurking nearby, of course, waiting for you to say or do something incriminating.

Threat #2 – A same-day response by the FBI means that surveillance might begin before you're ready for it. They'll catch you unprepared. The FBI surveillance team may end up watching you trying to hide the very material that you're hoping to conceal from them.

Threat #3 – The FBI's policy of managed aggression can easily provoke you into losing your temper, or your nerve, or both. It is a wicked strategy. That's why they use it.

It's easy to see why most people are easy prey for the FBI's surveillance machine. But it doesn't need to be that way.

Beating the FBI. There are people who routinely thwart the FBI. They know how to recognize the telltale signature of an FBI surveillance team. When they find themselves under surveillance, they use tactics that inhibit the FBI's ability to find out what they're really doing. They mislead the FBI.

These individuals make it difficult for the FBI to build a legitimate case against them. Perhaps even more important, they make it difficult for the FBI to build a *phony* case against them.

An individual like this is called a *hard* target. That's spy-talk for a surveillance target who knows what he's doing.

The methods and techniques that these individuals use are called *countersurveillance*. This article reveals some of those methods and techniques. Simply put, the article you are reading is about countersurveillance methods that will beat the FBI.

What you'll learn in this article. The article is comprised of two parts. The first section deals with FBI general strategy. You'll learn about the structure and underlying principles of FBI surveillance. They've been at this game for many years and they've learned many lessons. The second section of this article deals with specific tactics of FBI surveillance teams. A case study is utilized to explain and illustrate FBI behavior. It is based on direct experience and on information from confidential sources.

What you need to know about the FBI...

They are masters of the game. If you have something to hide, FBI surveillance could be the beginning of the end for you. Do not make the mistake of underestimating the capabilities of an FBI surveillance team. They are persistent. They are methodical. They are thorough. And they are fanatical about their work.

Drawing from decades of experience, FBI surveillance strategy has evolved into an advanced system that exploits the classic military principles of space, time, and force. This strategic foundation is present in every major surveillance operation run by the FBI. This foundation relies on the three pillars of rapid response, multi-layered teams, and managed aggression. While each of these is a serious threat to the target of a surveillance operation, the most deadly of the three is the multi-layered team.

Multi-layered teams...

The FBI's deployment strategy is insidious and conniving, yet brilliant. Because of the manner in which FBI agents are deployed, it is almost impossible to catch the FBI unawares during a surveillance operation. They always have a fall-back position. This is called the strategy of surveillance-in-depth.

Here's how it works. For most surveillance operations, the FBI actually puts two teams in the field. That's right. Two teams.

The first team is expendable. That means if it is *blown* (that's spy-talk for detected), the surveillance operation will still survive and reach its objective. This first team is called the *Decoy and Diversion Team*. In this article we will refer to it simply as the *Decoy Team*.

In surveillance operations involving *hard targets*, the Decoy Team expects to get caught. In surveillance operations involving *soft targets*, they expect to remain undetected in 75% of all cases. (A *soft target* is a person who has no countersurveillance skills or training, and is not on the lookout for surveillance.)

Any target who is alert – and on the lookout for surveillance – will eventually detect a *pavement artist* of the Decoy Team. *Pavement artist* is spy-talk for a member of a surveillance team that is watching you in public places. They are on foot and they are in vehicles.

At the same time that the Decoy Team enters the situation and begins surveillance on you, a second team also enters the game. This second team quietly slips into the environment, where it does its best to blend in with the background. This second team is called the *Stealth Team*. At the beginning of the operation, the Stealth Team makes no effort to watch you. Its only objective is to establish its presence – and to remain undetected.

This deployment strategy is incredibly effective. Here's why. The first team provides cover for the second team's arrival. Even a hard target is likely to be too busy watching the first team to notice the arrival of the second team. And when both teams are in place, you usually only notice the first team.

The top priority of the first team (the Decoy Team) is to see *everything* you do. They want to learn your habits and your daily routine. They don't want to be detected, of course, but they are prepared to pay that price if that is what's required in order to make sure they see absolutely everything you are doing. Their first priority is to acquire as much data about you as possible.

If you do detect the Decoy Team – and if they realize you've spotted them – the Decoy Team simply suspends its operations. They realize that you'll notice their departure. In fact, they're counting on it. They also realize that very few people will realize that a second team has blended into the background.

This second team – the Stealth Team – doesn't need to see everything you do. They have been briefed by the first team. The Stealth Team only needs to watch you during certain times and at certain locations where they think you might be up to something. The top priority of the Stealth Team is to remain undetected. And they are prepared to leave you unwatched for brief periods in order to retain their invisibility. This is called *picket surveillance* by the FBI, named after the gaps in a picket fence.

This two-stage approach to major surveillance operations is brutally effective. It has led to the ruin of many people who thought they could outfox the FBI.

Tradecraft. The undercover agents of the Stealth Team use

methods that are more sophisticated than those used by the Decoy Team. These methods are called *tradecraft*.

The Stealth Team is much more difficult to catch than the Decoy Team. You need to know what you're doing. It is vital that you do not let the Stealth Team realize that you've spotted them. That's because the best way to beat them is by feeding them misinformation.

The difference in methods used by the two teams is best explained by example. Numerous situations are described in the case study later in this article.

Layered surveillance. This concept of multi-layered surveillance teams is the backbone of the FBI's surveillance strategy. They almost never lead with their best team. They always hold something back so that they have a fallback position. This strategy is also carried over into other FBI operations.

When the FBI is trying to infiltrate an agent into your circle of friends, associates, coworkers, and acquaintances, they'll often use an expendable agent first. This first agent is a *Decoy Agent*, meant to provide cover for the infiltration by the second agent (the *Stealth Agent*).

If the first agent manages to penetrate your organization undetected, the FBI is delighted. But if he runs into difficulty, he is withdrawn. The second agent – who has blended into the background – is brought into play.

Why the FBI loves your lawyer. It is important for you to realize that most lawyers have no training in countersurveillance. This is unfortunate. When the subject of an investigation first realizes he is being "followed", he is angry – and outraged at the invasion of his privacy. In many instances, one of the things he'll do is complain to his lawyer about being "followed". Many lawyers advise their clients to "confront" the person who is "following" them.

They don't realize that this is a game for foxes, not pit bulls.

The lawyer's advice plays right into the FBI's hand. When the subject attempts to confront the surveillance team, the FBI simply drops back into stealth mode. The Decoy Team suspends its surveillance activity.

Because members of the Decoy Team are relatively easy to detect, their absence is easily noticed. The subject assumes that his lawyer's advice has achieved the intended effect. After all, the subject confronted the people who were "following" him and they immediately "stopped".

What the subject does not realize, of course, is that the Stealth Team is now active. They have been there all along, of course, as part of the background while the Decoy Team was working. When the Decoy Team departs, the Stealth Team is still there as part of the background. So from the subject's point of view, everything appears to return to normal.

Basic psychology. The FBI surveillance team is only too willing to accommodate your emotional desire for control over your immediate environment. It is a fantasy that will lead to your ruin. Here's why. When you see the Decoy Team has departed, you begin to feel safe, so you let down your guard. You become easy prey for the Stealth Team. Of course, infiltration comes next – FBI agents penetrate your circle of friends, associates, coworkers, and acquaintances. Arrest and indictment are simply a question of time.

Dummy up. Here's what this means in simple language. You can play the macho man OR you can beat the FBI. You cannot have it both ways. It is an "either-or" situation. If you insist on being a *know-it-all* tough-guy confronting the people who are "following" you, the FBI is going to play you like a cheap fiddle at a country hoe-down. To beat the FBI you need self-control and self-discipline.

Be smart. Learn from the mistakes of others. FBI surveillance teams do not just go away.

You don't stop wrestling a gorilla when *you* get tired. You stop when the *gorilla* gets tired.

NOTE – There is more to multi-layered teams than we cover in this article. The FBI often uses surveillance as an end in itself. As a method for suppressing dissent, criticism, and activism, nothing is more effective than letting the target know that he's under surveillance. Fear is a powerful tool. To get the big picture on surveillance – and to learn more about the mind-games the FBI plays – return to our home page and click on *Learning the basics*.

Rapid response...

This is the second component in the FBI's three-pronged strategy of multi-layered teams, rapid response, and managed aggression.

The width and breadth of the FBI's presence has been a closely-guarded secret up to now. Many people do not realize that the FBI can provide same-day response *anywhere in North America*. This is called the strategy of surveillance-in-time.

In fact, the FBI can mount a *same-day* surveillance operation in any city located in the United States, Canada, or Mexico. The FBI can also mount a same-day response in many major European cities, most major South American cities, and some Asian cities.

They use a skeleton crew to start. Outside North America they sometimes farm out the work to subcontractors.

Then, in many cases, the full surveillance deployment arrives overnight and begins work the next day. In situations where FBI resources are already stretched by other major cases, it may take two days for the full surveillance compliment to arrive.

But make no mistake about it, surveillance has been underway since day one. If they choose to do so – and they often do – the FBI can initiate surveillance the same day they become aware of you.

The reconnaissance factor. In many surveillance situations, a special team is deployed to provide reconnaissance information for the main surveillance teams. This reconnaissance team is called the *Advance Team*. The reconnaissance team is deployed ahead of the Decoy and Stealth teams that were discussed earlier in this article.

The Advance Team is tasked with establishing roughly who you are, where you are, and what you're doing. They'll take photographs of you, your home, your office, and your vehicles. The photographs help agents identify you on sight. The person who secretly takes pictures of you is called a *peep*. The peep often arrives at your doorstep disguised as a volunteer collecting for charity or as a religious canvasser. (Like the CIA, the FBI is big on using organized religion as cover for covert operations.)

Surreptitious entry. The primary task of the Advance Team, however, is to break into your office or home. This is called *surreptitious entry* by spies. That's just polite talk for break-and-enter. The break-in usually happens during the first few days of a surveillance operation.

Once inside, they perform a quick search of your property. They've got special ways to get inside locked drawers and office safes. (See future articles in *Spy & CounterSpy* for more on this.)

They'll often bug your office or home. Being able to hear all your conversations gives them a tremendous advantage. If they already know where you're going, it makes it easier to "follow" you. If they know you're going to a restaurant, for example, they can arrive "before" you do. The FBI's tactic of being the first to arrive at your destination has fooled many people over the years.

They'll also usually attach a tracking device (called a *beeper*) to your vehicle. This makes it easier for them to track you in traffic.

Clearly, if you are sharp enough to detect the Advance Team – and if you don't reveal that you've spotted them – you can enjoy a major tactical advantage over the FBI during the entire surveillance operation. You can either cloak your activities so they find nothing. Or you can feed them misinformation. (See future articles in *Spy & CounterSpy* for more on detecting the first break-in.) You can also watch the behavior of the surveillance team itself for telltale signs that indicate they've got your home or office bugged.)

Consequences of same-day response. What's the lesson in all this? Here's a real-world example. Suppose you are a controversial activist group. If you send out a news release to the media exposing government abuse, then you'd better be prepared for same-day surveillance by the FBI.

Not tomorrow. Not in a few days. Today.

The same advice applies if you are an investigative journalist submitting a controversial article for publication.

The implications of same-day surveillance can be serious. Suppose you've got documents or materials that you relied on when writing your news release or your article. These documents might contain references to confidential sources or informants or whistleblowers. You don't want the FBI to find these materials. You don't want to compromise your sources.

The materials had better be securely stowed away BEFORE you send out the news release. Trying to hide the materials AFTERWARD may be too late. Because if you think you're faster than the FBI, you're asleep at the wheel, heading for Dead Man's Curve. But be careful where you hide the materials. Safes, alarm systems, even bank safe-deposit boxes are generally useless against a determined FBI surveillance team. (Future articles in *Spy & CounterSpy* will describe how to keep information from the FBI. It isn't easy, but it can be done.)

The FBI's capability for same-day response has caught many surveillance targets unprepared. This is not a game for slowpokes. If you don't move fast, you're gonna be roadkill.

Managed aggression...

This is the third component in the FBI's three-pronged strategy of multi-layered teams, rapid response, and managed aggression.

The FBI has a bureau-wide policy of managed aggression. This policy also affects FBI surveillance operations.

Surveillance teams are given specific goals. The FBI command structure accepts no excuses. It tolerates no failures. This strategy of surveillance-for-results leads to aggressive behavior in FBI surveillance teams because of the pressure they're under. This results-driven aggression tends to manifest itself as professional aggression.

An FBI surveillance team is using professional aggression when it intentionally and deliberately applies pressure to the subject of a surveillance operation. Actions like this are called *psy-ops*, which is spy-talk for psychological operations.

Here is an example of how an FBI surveillance team will deliberately provoke you.

When you're walking through a mall or a downtown shopping district, the surveillance team will intentionally interfere with your route. A pavement artist will "absent-mindedly" cross your path, forcing you to change course to avoid walking into him. A group of agents will "inadvertently" obstruct your path – they'll be standing together chatting, forcing you to walk around them. Other pavement artists will "accidentally" create near-misses as you walk along. Some of these "pedestrians" will create situations with a potential for a head-on collision, forcing you to dodge them.

As the psychological pressure continues to build, agents may "innocently" bump into you, jostle you, or step on your heel from behind. A group of pavement artists will cue up ahead of you, creating a line-up that delays you as you try to make a purchase, order fast food, buy tickets, and so on.

Activity like this can quickly create frustration, even anger, in you. But because the incidents occur in public locations, it's difficult to prove who's behind them. You never see any agent more than once. You don't know where the next provocation is going to come from. You're beginning to get upset, irritated, unstable. You're more likely to make mistakes in judgment. And that's exactly what the surveillance team wants.

When a surveillance team is experiencing difficulty cracking open an investigation they sometimes resort to professional aggression. This is a wicked mind-game. It can be very effective if you're not anticipating it. The FBI surveillance team has the power to make or break your day – and they don't hesitate to use that power.

This is not a game for choirboys.

NOTE – There is more to managed aggression than we cover in this article. For more on mind-games the FBI plays, return to our home page and click on *Learning the basics*.

Conclusions: FBI surveillance strategy...

The FBI's triple-threat surveillance strategy of multi-layered teams, rapid response, and managed aggression must be taken seriously. These three threats were mentioned at the beginning of this article. They are important enough to be repeated.

Threat #1 – A multi-layered team can fool you into thinking that the surveillance has ended. This is an extremely dangerous situation. They're still lurking nearby, of course, waiting for you to say or do something incriminating.

Threat #2 – A same-day response by the FBI means that surveillance might begin before you're ready for it. They'll catch you unprepared. The FBI surveillance team may end up watching you trying to hide the very material that you're hoping to conceal from them.

Threat #3 – The FBI's policy of managed aggression can easily provoke you into losing your temper, or your nerve, or both. It is a wicked strategy. That's why they use it.

Case Study:
Beating an FBI surveillance team...

The preceding discussion provided the background knowledge

you need to begin beating the FBI. But the real value of this article lays in the section you're reading now – the case study. That's because the case study is based on actual events.

The background. The author resides in a city where a joint USA-Canadian defense research facility was located. It developed anti-submarine warfare systems. This meant a community with active espionage and surveillance operations.

The author was under hostile surveillance for eight years. (See About Us for more on this.) In order to strengthen his countersurveillance skills, the author hit on the idea of provoking other agencies into conducting surveillance against him. Much like the way hackers break into computer systems, the author hacked surveillance operations.

The situation. The author sent a letter by commercial courier to the head of counterintelligence at FBI headquarters in Washington DC. The letter offered to provide information about the countersurveillance capabilities of the FBI's adversaries.

The following discussion describes part of what happened next. The case study is a compilation of incidents that occurred during surveillance operations mounted by the FBI over a one-year period.

The incidents have been organized into four episodes for easier reading. Events are reported in the present tense using the first person singular. This reporting style provides a more authentic portrayal of what it feels like to use countersurveillance in an adversarial environment.

Case Study section begins...

The setup. Before sending the letter, I establish a personal routine that makes it easier for me to detect surveillance. When driving, I choose the same times along the same routes. I select busy streets and quiet streets. I study the timing of traffic lights. I observe the driving habits of other motorists. I learn vantage points where observers might lurk.

Then I go through the same exercise for my pedestrian routes.

I establish a lifestyle that will capture the attention of a surveillance team. I want them to focus on certain aspects of my behavior. I choose social activities that offer situations where spies will suspect "secret contacts" are taking place. I study the venues, people, and events that are normally part of these situations. I begin to fit in.

I become a creature of habit at home and at my office. I store items in particular ways. I allow dust to accumulate in some locations, while others are kept meticulously clean. I hide mildly incriminating documents for the FBI to "find". I tune myself to the feel of the locks in my life – doors, desks, filing cabinets, office safe, personal vehicle, and so on.

My goal is to know my environment. I want to be able to detect the arrival of the surveillance team – no matter how silently they stalk their prey.

Episode 1: Reconnaissance – The FBI's Advance Team

To get the big picture on surveillance – and to put this Case Study into perspective – return to our home page and click on *Learning the basics*.

Day Zero, 1:00 pm, Wednesday afternoon – The FedEx? truck arrives to pick up the letter. I've already got the waybill prepared. For $24.50 they guarantee next-day delivery. The driver tells me I'm his last pickup on his way out to the airport. My package will be going out on the 1:30 flight.

Day One, 2:00 pm, Thursday afternoon – I call FedEx and I ask about package 400-7033-0341. The package has been delivered. My letter is now in the hands of the Assistant Director, National Security, Federal Bureau of Investigation, #7110 – 935 Pennsylvania Avenue NW, Washington DC, 20535-001.

4:30 pm, later that afternoon – I decide I'll go out later for the evening. I won't have that many more chances to relax. It's already Thursday. I'm expecting surveillance to begin Monday.

9:15 pm, later that evening – After a meal at The S----- ------ restaurant downtown, I'm driving out to The W------, a working class bar in the suburbs. They've got karaoke on Thursday nights. The crowds they get there love classic rock and country. That suits me fine. I like to sing rock'n'roll.

As I turn left off Gorge Road onto Admirals Road, something behind me catches my attention. This is normally a quiet stretch of

road this time of night. It's early March, too dark to see anything but headlights. The vehicle behind me is maintaining a constant distance.

Unusual. Most motorists drive 5 or 10 mph over the limit here.

"Unmarked police car," I tell myself. I glance at the speedometer. Bang on the legal limit. I make a note to watch my driving habits anyway.

A mile later I go through a choke-point and merge onto Sooke Road. My follower turns away. He is replaced by another vehicle maintaining a fixed distance. After years of surveillance I see things like this. I can't turn it off any more.

"That's not how traffic cops work," I caution myself.

I don't have enough data yet, but I'm already figuring somebody might have me under surveillance. But who? I don't want any third party messing up the ambush that I have laid for the FBI.

10:15 pm, same evening – Two songs later at The W-------. The place is only half full, but it's rocking. There are 60, maybe 70, people in the place. A swarthy mixture of working-class folks, with a sprinkling of biker types. A rough crowd, but good people at heart. You get the picture. They don't put on airs or dress up. Hey, when you do what I do, you learn to fit in anywhere.

I'm sitting with a couple of women at a table at the far end of the room from the entrance. The karaoke stage is to my right. The music is loud. The place smells of beer and sweat. A honky-tonk kind of place. Between singers the MC is doing a pretty good job working up the crowd.

A thirtyish guy walks in – physically fit, clean shaven, a trim haircut, slacks, brown leather Bomber jacket, slightly overdressed for the joint. He looks the place over. He doesn't make eye-contact, but he seems to be keying on me. He chooses a seat that gives him a clear line-of-sight – right to where I'm sitting with Diana and Kimberley.

I make a note to myself. Run some surveillance tests tomorrow. I hear the MC calling my name over the speakers. My song is up next. Okay, now we rock, I tell myself.

Day Two, 10:30 am, the next morning – It's a nice sunny day. It seldom gets cold enough for snow here. I decide against going into the office. Instead I plan to go downtown, pay a few bills, pick up mail at the PO box. I'll use routes that will provide opportunities to check for surveillance – vehicle or pedestrian, or both.

Instead of taking a direct route over to the mall on Hillside Avenue, I take the long way around. I drive through Mt. Douglas Park. It's picturesque and rugged – full of old Douglas Fir trees. Fists of gray rock thrust up through the moss that covers the forest floor.

The main road through the park snakes along the sea coast. There's a straight stretch, though, notorious for speeders. But I'm in no hurry. The sun is flaring through the fir trees, blasting lines of shadows across the road like zebra stripes. It's hypnotic. I check the mirror. The vehicle behind me is holding the same fixed distance since before I entered Mount Doug.

I can't help thinking about last night. Same style, same team? Hmm. Am I beginning to see a pattern? I warn myself about jumping to premature conclusions.

10:55 am, same morning – Inside the mall, I head for B---- Books. They've got a good selection of computer books. I zero in on the titles for programmers. I used to write this stuff myself and I'm still interested in it.

Then I get my first break. (I don't mind admitting that it cuts both ways – you have to be lucky to be good, and you have to be good to be lucky.)

I've been on the lookout for signs of foot surveillance, but I haven't seen anything odd yet. The book store is relatively quiet – maybe twenty customers in the place, and it's a sizable place. There are two or three other customers near me, but they're a few aisles over, either behind me or in front.

A woman, thirtyish, plain, walks in and comes over to the section I'm in. She's checking out books at the end of my aisle, about four or five paces from me. She squats down to go through the titles on the bottom row. I've seen this squatting behavior before in spooks – they use it to throw you off by changing their profile, appearing less threatening. But that doesn't mean everyone who squats is a pavement artist. By itself, it means nothing. It only counts if it's part of a larger pattern of behavior.

But while I've been watching her, a male has arrived behind me.

He's about three paces away. He's wearing a businessman's suit and tie. You don't see many programmers wearing suits.

The clerk catches him completely off guard. She approaches from behind. She offers to help him find whatever he's looking for. In fact, she insists on it. She proceeds to engage him in conversation.

And he chokes. Big time.

He doesn't know anything about programming. Or computer languages. Or applications. Absolutely zip. Nuttin' at all. And the more the clerk presses him, the less he knows. I can't believe my good luck.

Keep in mind there's maybe twenty people in the whole place, spread out evenly throughout the book store. Except for the section on computer programming books. Where there are now four of us crammed together.

And I'm starting to consider all the angles. Hmm, if the squatting female was an agent, maybe she was providing cover for the male. It takes resources to run operations like that. Could this be the FBI? Already? Did they initiate surveillance last night? The same day they received the courier package?

Aw, come on. Nobody's that good.

I've seen enough here. I leave the book store. I head for my car. I've got some errands to take care of downtown. Besides, I need more empirical evidence before I can draw any conclusions. What happens next is a jolt. Literally.

11:20 am, same morning – I pull out of the mall parking lot, turn right on Hillside Avenue, and point my Mazda? 626 towards downtown. Two miles down the road I ease into the left-turn lane as I approach Quadra Street.

The light is red. I come to a full stop.

The car behind me doesn't.

It's a mild collision – the impact is barely stiff enough to skid my car ahead a few inches. I glance at the mirror. Two young fellas, laughing, kidding around – not paying as much attention as they should.

Off comes the seatbelt and I'm out of the car, stepping around back to check for damage. The driver pokes his head out the window. He's still laughing. He apologizes, says he hopes there's no damage. He's the friendly type, all smiles, genuinely sorry. Hey, how can you not like a guy like that?

I can't see any damage. I spin on my heels and head back to my car. He yells out another sorry. I toss him a *no-hard-feelings* wave as I slide back into the Mazda.

The light flips green. I turn left onto Quadra. I'm already replaying it in my head. Was there any way I could have avoided the collision? Maybe slow down a little earlier? Give him a little more warning?

The driver in front of me slows to make a left turn. He hesitates, changes his mind, and proceeds straight on. At the next corner he slows again. Same thing. What's wrong with this guy? Finally, at the third corner he makes his left turn. Good riddance, jerk.

A few blocks later – it's another idiot. He can't decide which lane he wants. He starts to change lanes, goes back, ends up straddling both. Get out of my way, dolt.

Then – zzzap!

"Look at all the lousy drivers I'm encountering," I think to myself. Yeah, right.

Right after I left the mall. Right after the book store thing. Right after the spook in the book store *had his cover blown by the clerk*. With me standing next to him.

Nasty traffic. Yeah, right. *They're trying to recover from their blunder*. This traffic stuff is a diversion. They're trying to salvage their surveillance operation. They hope to distract me – force me into a different mind set – stop me thinking about what happened in the book store.

Professional aggression, I'm telling myself. I've seen it in other surveillance teams. Usually not this rough, though.

The trick is to detach yourself from what's happening to you. Then you can put it in perspective. Most targets would still be fuming over the collision. And would have completely forgotten the book store incident.

These guys are good, I tell myself. Very good. We're talking advanced psychology here.

I remind myself not to leap to hasty conclusions. But if I'm right – and I'm beginning to think I am – if indeed this is a surveillance

operation – then I can expect to start seeing more of the pattern.

As I begin to enter the downtown section of the city, I steel myself for what's coming next. Whoever they are, these guys play for keeps. I cannot rely on luck anymore. The book store thing was a freak event. I need to make my own luck.

It's time to begin using active countersurveillance.

Coming up next in the Case Study...

In Part 2 of the Case Study you'll learn how the pavement artists of the FBI advance team were detected while the author was running errands downtown. You'll see the countersurveillance technique he used to provoke a response that betrayed the presence of the surveillance team.

Arriving back home, the author was able to detect circumstantial trace evidence of a break-in. You'll see how he systematically and meticulously laid the groundwork for exposing the existence of bugs in his office and in his home.

Then you'll see how the author unmasked the *peep* – an FBI photographer tasked with building a dossier enabling other FBI agents to recognize the author on sight.

In Part 3 of the Case Study you see the FBI Decoy Team enter the game and take over the surveillance operation. You'll see how the author picks apart their operation, exposing their stakeout tactics, revealing the covers that their agents use, and detecting their observation posts.

In Part 4 the Decoy Team withdraws and the Stealth Team takes over. The author shows you the differences between the two surveillance operations. You'll learn how to see through the veil of deception used by the FBI.

Future articles in *Spy & Counterspy* will expose the tactics that the FBI uses for infiltration and penetration. You'll learn about the two-stage and three-stage setups that have led to the ruin of many surveillance targets.

Back to Home Page

---

your requirements, or that the performance of the methods will be error-free, or that delivery of the product will be uninterrupted or error-free, or that defects in the product will be corrected. Furthermore, *Here's-how, Right-now! Seminars Inc.* does not warrant or make any representations regarding the use or the results of the use of the product or related documentation in terms of their correctness, accuracy, reliability, or otherwise. No oral or written information or advice given by *Here's-how, Right-now! Seminars Inc.* or its authorized representatives shall create a warranty or in any way increase the scope of this limited warranty. Should the product prove defective, you (and not *Here's-how, Right-now! Seminars Inc.*) assume the entire cost of all necessary correction, repair, or servicing. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. *Here's-how, Right-now! Seminars Inc.* shall not be liable for special, incidental, consequential, or other damages, even if *Here's-how, Right-now! Seminars Inc.* is advised of or aware of the possibility of such damages. This means that *Here's-how, Right-now! Seminars Inc.* shall not be responsible or liable for lost profits or revenues, or for damages or costs incurred as a result of loss of time, data, or use of the product, or from any other cause. In no event shall *Here's-how, Right-now! Seminars Inc.*'s liability exceed the purchase price of the product. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. The author and publisher of the product have used their best efforts in preparing the product and the material contained in it. These efforts include the development, research, and testing of the theories and methods in order to determine their effectiveness. The author and publisher make no warranty of any kind, express or implied, with regard to these techniques or the documentation contained in this product. The author and publisher shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of the techniques, associated instructions, and/or claims of productivity gains.

Security software...

Updated October 22nd, 1998.

SPY & COUNTERSPY

What the FBI and IRS don't want you to know – Your hard disk is more incriminating than a daily diary if you fail to clean it regularly.

Why the authorities love your computer. Most people don't realize how easy it is to recover incriminating data from your computer. Even a local sheriff's department has software for snooping around your hard disk. Here's what they can do.

1. They can recover files *you thought you erased*.
2. They can recover files *you thought were overwritten*.
3. They can recover files *created without your knowledge*.
4. They can recover remnants of *the Windows swap file*.
5. They can recover names of *Internet sites you visited*.
6. They can recover *your old email messages*.

Secret temporary files. You probably didn't realize that every time you print a document, Windows writes a temporary copy to disk. It "erases" the file when it's finished, but an *undelete utility* can recover the file.

Secret swap file. Windows creates this file whenever memory gets tight. Investigators can often recover documents, data, personal information, and passwords from months ago. A *binary sector editor* can view the data in the swap file, often named *win386.swp*.

SECURITY TIP – Many notebook and laptop computers use a hibernation file to save the contents of RAM when the rechargeable battery runs low. You'll want to delete, shred, and recreate this file. For example, if you're using an IBM *ThinkPad*, look for a file named *pm_hiber.bin*, in addition to the Windows swap file.

Try it for yourself. See for yourself what investigators can find on your computer. You can download a free demo copy of Expert Witness™, a forensic data acquisition program for Windows 95 at http://www.guidancesoftware.com. This is the same software cops use. It's got a point-and-click interface that anyone can learn to use. It allows sector-by-sector viewing of your hard disk, including hidden files, previously "erased" files, the Windows swap file, unallocated disk space, and file slack (the space between the end of the file and the end of the cluster). The software provides a record of the *chain of custody* of the evidence (that's polite talk for the data on your computer). The software can even save *your entire hard disk* as evidence.
(NOTE: Spy & CounterSpy is not affiliated with this product.)

Protect yourself...

Spy & CounterSpy recommends that you take a methodical approach to sanitizing your computer's hard disk.

You may wish to consider downloading the following applications. Each is designed for use with Windows 95. Some of the names mentioned are trademarks.
(NOTE: Spy & CounterSpy is not affiliated with any of these products.)

Shredder: Shredder is designed to run in the background while you work with your personal computer. Shredder intercepts all disk accesses and *completely wipes a file* before allowing an overwrite. Shredder also *wipes the Windows swap file* at the end of each work session. This secures your system against undelete utilities and sector editors. You are safe from investigators who are using file slack recovery and Windows swap file readers.

SECURITY NOTE – It takes a much stronger magnetic charge to completely overwrite and obliterate a pre-existing charge. This is a polite way of saying that overwriting a file still leaves subtle magnetic traces of the previous data. Intelligence agencies and security services use magnetic force scanning tunneling microscopes to detect these traces. Shredder can protect against this threat. It can also protect you against investigators using an electronic microscope with spin detectors.

A very useful feature is Shredder's panic mode. If you're at your computer when the goons kick the door in, simply press your secret keystroke combination and Shredder instantly shreds a preselected list of sensitive files. Shredder will also get rid of any so-called history lists that your browser makes, as well as old email. You can download a free demo copy of Shredder from http://www.shredder.com.

HEdit: This hex file-editor is useful for inspecting the files on your hard disk. You can check both the hexadecimal and ASCII contents of any file, including the Windows swap file (named win386.swp on most systems). You can also use HEdit to alter the contents of any file on a byte by byte basis. To download a free trial version of HEdit, set your browser to

http://www.yurisw.com/hedit.

File Vault: This freeware program is ideal for encrypting groups of files on your hard disk. It can also be used to create standalone self-decrypting message files that you can send to correspondents by email. File Vault uses the Blowfish encryption algorithm, which is resistant to NSA attack. Included with File Vault are the DiskWipe and FileWipe utilities. DiskWipe scrubs the free space on your hard disk. FileWipe permanently erases a file so it cannot be read with either an undelete utility or a sector editor. To download File Vault, set your browser to http://www.alcuf.ca/fv.htm. You can also download an encryption-enabled text editor called VGP from http://www.alcuf.ca/vgp.htm.

PGP: Pretty Good Privacy is a public-key encryption program that uses a combination of prime numbers and one-way math functions. *When used correctly*, it provides strong protection for your confidential documents and email messages. You can use it to encrypt files on your computer. You can use it to send encrypted email to recipients you've never met. Or you can use it to digitally sign your email so recipients can tell if it's been tampered with. PGP is available in a variety of freeware and commercial versions in standalone configurations or as plug-ins for various email programs and word-processors. The US government restricts the export of this and other encryption software outside the USA and Canada. If you're in the USA or Canada, you can download the freeware version of PGP version 5.0 from http://web.mit.edu.network/pgp.html. The commercial version of PGP version 5.5 is available at http://www.pgp.com. The online user's manual tells you everything you need to know. PGP's international download site is found at http://www.pgpi.com.

Sam Spade: This freeware program is – for all intents and purposes – a *hacking toolkit*. Its powerful features give you the power to trace the source of spam email (and others who may have forged the header of the email message). You can also ping every server in a domain, sweep for IP addresses, and track down server ports. Some of these functions are considered to be a *crack attack* by the server administrators. You can download a copy of this hacker's dream-tool from http://www.blighty.com.

RPK InvisiMail: This shareware program provides *hands-free* email encryption. It sits between your email software and your ISP. The software automatically exchanges public keys with any of your correspondents who are also using InvisiMail. Otherwise, it sends out your email as plaintext. Invented by an American cryptographer, RPK was developed in New Zealand, outside the prying eyes of the FBI et al. Hence RPK is not subject to any heavy-handed export restrictions (or forced inclusion of *trap doors* for use by US Government spooks). InvisiMail is based on the RPK mixture generator, whose exponentiation math is as strong as PGP's. The patent-protected algorithm is available for inspection. (They're offering a US$10,000 reward to anyone who can crack RPK.) You can download a free-trial version of InvisiMail from http://www.invisimail.com or http://www.rpkusa.com.

BCWipe: This is a freeware program that does three things. First, you can use it to permanently erase files so they can't be recovered by so-called undelete utilities. Second, you can use BCWipe to clean the free space on your hard disk. And, third, you can use it to wipe the Windows swap file on your hard disk. Wiping the swap file is important. Personal data and passwords from three months ago can still be sitting there. The FBI and IRS routinely recover a significant amount of evidence from suspects' swap files. To download BCWipe, set your browser to http://www.jetico.sci.fi/bcwipe.htm. Simply run the downloaded .exe file to install the software.

Here is the small print. It appears here because we have found that maintaining a corporate front is the only way we can protect ourselves against interference by governments and their agencies. The legal underpinnings of our corporate front are our first line of defense against audit-attacks and other methods of economic warfare that the authorities use to suppress dissent, protest, and activism. They are also determined to prove their hypothesis that *Spy & CounterSpy* is funded by a foreign intelligence agency or terrorist group – but our double entry accounting record of corporate revenue and expenses is our shield against fabricated evidence by an overzealous investigator or case officer.

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com

About Us...

This page describes our organization and the three main participants – Lee Adams, Vickie Nickel, and Agent X.

Spy & CounterSpy is published by Lee Adams Seminars.

Lee Adams Seminars is a division of *Here's-how, Right-now! Seminars Inc.* with offices at 3273 Tennyson Avenue, Victoria, BC, Canada. The company was founded in 1994 by Lee Adams.

His original goal was to provide business skills training – in the methods of personal persuasion he had learned during a decade of encounters with some of the world's most sophisticated intelligence agencies and security services.

In 1998 he expanded the company mandate to include publishing information about countersurveillance.

About Lee Adams...

Lee Adams first came to the attention of the authorities during a routine check by a joint US-Canadian top secret research facility to renew his access clearance. Using the thinking skills he had honed while writing computer programming books for McGraw-Hill, he quickly became adept at spotting the spies and their methods.

When he took his concerns to the authorities, he was rebuffed. But the surveillance immediately intensified. Lee Adams found himself in the role of *crash-test dummy* as the spies attempted to upgrade their methods. But while they were watching him, he was watching them. They were inadvertently showing him their best stuff.

Faced with unremitting surveillance, he wanted to learn as much as he could about his adversaries and their methods, so he hit on the idea of provoking other groups into watching him.

The subsequent knowledgebase and contacts that Lee Adams built during 8 years of surveillance is the backbone of *Spy & CounterSpy*.

About Vickie Nickel...

Vickie Nickel is the subscription manager for *Spy & CounterSpy*. She is a former high-ranking civilian employee of the *Canadian Armed Forces*. Most recently, she was D/Admin (that's *bureaucrat-talk* for Director of Administration) at a *Defense Research Establishment* on the west coast. She reported directly to the Chief of the top secret facility.

The facility was a joint project of the US and Canadian military. The research focused on antisubmarine warfare. The scientists worked in close partnership with a similar facility located in San Diego, CA. The facility was a prime target of Soviet military intelligence.

Vickie was put under 24-hour a day surveillance during an attempt by the authorities to unmask Soviet agents. She became increasingly frustrated at what she calls the *"stupidity"* of the surveillance team as it interfered with her ability to maintain a normal lifestyle. The surveillance team found no incriminating evidence because there was none.

After four years of surveillance, the authorities finally acknowledged what Vickie had been trying to tell them all along – she had been set up. Soviet military intelligence had framed her, in order to divert attention away from the real moles – and US Naval Intelligence had swallowed the bait. Disgusted with what she calls *"the senseless damage"* caused by inept surveillance and a bungled investigation, Vickie resigned after 21 years' service rather than accept a posting to military HQ in Ottawa.

About Agent X...

Agent X is not one agent, but *three*. Agent X is our name for

SPY & COUNTERSPY

Agent A is not one agent, but *three*. Agent A is our name for what is actually a *composite* of three people – our three confidential sources in the intelligence community. We rely on these individuals to help us in two important ways.

First, they confirm the conclusions that we have reached through direct observation, by deductive reasoning, and by abductive reasoning.

Second, they provide hints and tips – new leads for us to investigate, new countersurveillance techniques for us to evaluate, new perspectives on what is being reported in the mainstream news media about intelligence and security matters.

Confidential Source #1 – is a former DST case officer. The DST is France's security service. Our source also liaised closely wth the police intelligence apparatus, *Renseignements Generaux*. After 32 year's service he retired and began to write his memoirs. When he began approaching publishers he found himself narrowly averting vehicle collisions in traffic, pedestrian hit-and-runs, and other lethal situations. He quietly investigated and learned that other ex-officers intending to publish had all died in accidents. He has since found another way to publish – by acting as a clandestine consultant to *Spy & CounterSpy*.

Confidential Source #2 – is a former SIS agent. The SIS is Britain's secret intelligence agency. Our source spent a number of years working closely with MI.5 during its penetration of IRA cells in Northern Ireland. He also liaised frequently with CIA and FBI teams during attempts to obstruct IRA arms shipments from the USA. He spent 4 years in deep cover in the United States and Canada tracking IRA fundraisers. He became disillusioned with what he calls the *"extra-judicial execution of Irish civilians"* during sweeps by the British authorities – and the coverups that followed. He has declined to discuss with us whether he subsequently provided intelligence to the IRA.

Confidential Source #3 – is a ex-cadre with the *Shining Path*, formerly the primary guerrilla group in Peru. Our source emmigrated to North America a few years ago when the Peruvian authorities arrested the Shining Path's leader. She is familiar with methods and techniques for maintaining cells in an adversarial urban environment. She claims to have contacts with underground movements in Uruguay (the Tupamaros?) and Argentina (the Montoneros?). Our contact with her is intermittent and through an intermediary, so it is difficult for us to verify her story. Her information so far has been found to be reliable. We have tested the methods she has provided and found them very effective for operating undetected in urban settings.

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com

Archive of News Releases

Updated: September 2nd, 1998
News releases archived: 8

The following news release was distributed September 2, 1998 by fax and email to 282 news media organizations and journalists in the USA, Canada, and UK.

News Release

For Immediate Release

FBI "wheel artists" exposed.

VICTORIA BC, CANADA – September 2, 1998 – Between 250 and 400 people a day are receiving countersurvellance training from a free Web site in California that bills itself as *spy school for the rest of us*.

Since February, a spy watcher in Canada has been using the Internet to expose the methods used by the FBI to suppress protest and dissent in the USA. The current focus is on FBI vehicle surveillance teams.

"They call them *wheel artists*," says Lee Adams. "But that's just spy-talk for a surveillance agent in a vehicle."

"They don't follow you – they surround you," he says. "They become part of your environment. You never see the same vehicle twice. Up to twenty FBI agents at any one time. Even more if the investigation involves national security."

According to Adams, the FBI trains its agents in the use of the *floating-box system* of vehicle surveillance.

"The surveillance team creates a box of vehicles around you," he says. "The box floats with you as you travel along your route. Hence the name floating-box."

Adams is using his Web site at *http://www.spycounterspy.com* to expose the tactics and diversions that FBI agents use to avoid detection by the people they're watching.

A typical FBI vehicle surveillance unit is composed of sedans, coupes, stationwagons, pickup trucks, vans, minivans, sport utility vehicles, taxis, motorcycles, commercial trucks, ambulances – even 18-wheelers, according to Adams.

"They'll even put a surveillance vehicle on the road *ahead of you*," he says.

"When the vehicle that is watching you is in front of you, they call it a *cheating* surveillance vehicle. They fool a lot of people with that one."

Adams says he has no plans to discontinue publishing his disclosures at his Web site at *http://www.spycounterspy.com*

The following news release was distributed June 12, 1998 by fax and email to 121 news media organizations and journalists in the USA, Canada, and UK.

News Release

For Immediate Release

FBI reads encrypted email.

VICTORIA BC, CANADA – June 12, 1998 – A spy watcher in Canada says FBI surveillance teams routinely crack encrypted email.

"PGP is a good example," says Lee Adams. "It's a first-rate encryption program – but most people aren't using it correctly, mainly because they don't understand how the FBI operates."

"FBI methods are based on two classic strategies. Some methods rely on the FBI's ability to get inside your home or office undetected. Other methods involve electronic equipment that can detect at a distance what's happening on your computer."

"Most people don't even realize they've been compromised," says Adams. "They continue to send email they think is confidential."

Adams is using his web site at http://www.spycounterspy.com to expose the different methods used by FBI surveillance teams.

"We explain ten methods," says Adams. "Six of those methods

involve surreptitious entry by the FBI. That's spy-talk for break-and-enter. Most people have a difficult time accepting that a surveillance team can get inside undetected – not just once, but many times."

"The FBI often needs to make repeated entries in order to pick through all your stuff," says Adams. "They've developed some fascinating methods for getting in – and we're finding that people are more serious about their privacy once they find out what the FBI has been up to."

The web site provides step-by-step instructions on how to prevent an FBI surveillance team from reading your confidential email.

"The first step is purely defensive," says Adams. "But once you've made it difficult for them to crack your email, you can go on the offensive. It's possible to use bogus email to detect the presence of a surveillance team you didn't realize was there. This method works against FBI and BATF teams. It's particularly effective against standard police surveillance."

Adams says he has no plans to discontinue publishing his disclosures at his Web site at http://www.spycounterspy.com

---

The following news release was distributed May 11-12, 1998 by fax and email to more than 100 news media organizations and journalists in the USA, Canada, and UK.

News Release

For Immediate Release

Spy watcher exposes Bureaucrats' Toolkit.

Methods for political control over the American people.

VICTORIA BC, CANADA – May 11, 1998 – A spy watcher in Canada continues to be a thorn in the side of the FBI by using the Internet to reveal suppressed information.

Lee Adams warns that government has recently been provided with the opportunity – and the means – to permanently wrest control from the population.

"We face three separate threats," he says. "Together these combine to give government a stranglehold on civil liberties – a death grip on traditional freedoms."

Threat #1 – Computers have taken over surveillance. Entire populations can be supervised and monitored automatically. Dataveillance makes it easy for government to track certain classes of people – like minorities or dissidents– or anyone who dares think for themselves. Databases and CCTV video cameras are to blame.

Threat #2 – The militarization of the police. The cops are now using some very nasty weapons. Half the stuff they use is prohibited by the Geneva Convention and the Hague Declaration. The government can't use it in war, but their own population is fair game – for CS and OC gas sprays, beanbag projectiles, new mark-free interrogation tools, and handgun ammunition that can amputate your arm or leg.

Threat #3 – Proliferation by private companies. Most of these high-tech gadgets are dual-use. There's no regulation or control over research, manufacture, export, and deployment of this nightmarish technology. The surveillance cameras in Tiananmen Square were exported from the USA as advanced traffic control – but they enabled China's dreaded Guoanbu security service to round up all the "troublemakers". Private companies are reaping huge profits in the newly-emerging police-industrial complex.

"These three conditions are being used by bureaucrats as a new technology for political control over people – not only in the USA, but worldwide," he says. "This information comes direct from a report commissioned by the European Parliament."

Adams says he has no plans to discontinue publishing his disclosures at his Web site at http://www.SPYCOUNTERSPY.com

---

The following news release was distributed April 1, 1998 by fax and email to 63 news media organizations and journalists in the USA, Canada, and UK.

News Release

For Immediate Release

Spy watcher continues to taunt FBI.

Internet site teaches activists to resist surveillance.

VICTORIA BC, CANADA – April 1, 1998 – A spy watcher in Canada continues to taunt the FBI by using the Internet to spread previously-secret information about countersurveillance to activists and dissident groups across the USA.

Lee Adams warns that any group questioning the status quo should consider forming a countersurveillance section.

"No matter how benign your goals you are considered a threat. Ipso facto you become a target for surveillance," says Adams. "The FBI uses surveillance for observation, infiltration, sabotage, and intimidation. Any one of these can stop your group reaching its goals."

"You need to learn to set up cells in your organization and make it resistant to infiltration by the FBI. Their agent-provocateurs can seduce you into reckless behavior. Their informants can ruin your operations."

"You need to learn to ensure the FBI can't arrest you on conspiracy charges," says Adams. "Conspiracy is the most common grounds for arrest when surveillance is involved."

"You need to learn a system of tactical communication. This means things like spoken conversations, facial expressions, gestures, and mannerisms that can be used to keep your communication private – even when under hostile surveillance. The world's top intelligence agencies are already using this system. Of course, the FBI doesn't want you to know about it."

Adams says his Web site is like spy school for the rest of us. "The only other people who could teach you this stuff are the spooks themselves. But they can't," says Adams. "They get prison sentences – or worse – for talking."

Adams says he has no plans to discontinue publishing his countersurveillance disclosures at his Web site at http://www.SPYCOUNTERSPY.com

---

The following news release was distributed March 25, 1998 by fax and email to 57 news media organizations and journalists in the USA, Canada, and UK.

News Release

For Immediate Release

Internet site teaches victims of FBI surveillance to cloak their actions.

VICTORIA BC, CANADA – March 25, 1998 – A spy watcher in Canada is using the Internet to provide countersurveillance skills to activists and dissidents in the USA.

"Our mission is to level the playing field by providing information to supporters of freedom, democracy, and fairness," says spy watcher Lee Adams.

"The FBI is more than a police agency," he says. "It is a security service. There are important differences between police agencies and security services."

"Every government has a security service. The mission of a security service is to suppress anti-government activity. The prime directive of a government is to stay in power. Most governments see their own population as a threat."

"The nastier the government, the nastier the security service," says Adams. "The FBI does not have a history of respect for civil rights in its role as a security service. The FBI protects the government from the people. The people have no such protection against the government."

Adams warns that any group questioning the status quo should consider forming a countersurveillance section. "No matter how benign your goals, you are considered a threat," he says. "You become a target for surveillance."

"A security service like the FBI uses surveillance for observation, infiltration, sabotage, and intimidation. Any one of these can stop your group reaching its goals."

"You can learn to detect surveillance teams," says Adams. "Even more important, you can learn to cloak your actions and carry on undetected even while you're under hostile surveillance."

Adams says he has no plans to discontinue publishing his countersurveillance disclosures at his Web site at http://www.SPYCOUNTERSPY.com

---

The following news release was distributed March 7, 1998 by fax and email to 50 news media organizations and journalists in the USA, Canada, and UK.

News Release

For Immediate Release

Spy watcher reveals how to beat FBI surveillance.
Activist, militia, civil rights, other groups on mailing list.

VICTORIA BC, CANADA -- March 7, 1998 -- A spy watcher in Canada is using the Internet to reveal the operating methods of FBI surveillance teams. Lee Adams says he is breaking no laws by telling what he learned by watching agents who were watching him.

"The FBI utilizes a triple-threat scheme of multi-layered teams, same-day response, and managed aggression," says Adams.

He claims that FBI surveillance strategy is built on military prinicples of space, time, and force.

"The FBI has been at this game for many years. They've learned many lessons," says Adams. "Their surveillance strategy has meant ruin for many people who thought they could outfox the FBI."

"Threat #1 -- FBI multi-layered surveillance teams play a classic scam. They lure you into thinking surveillance has ended. But they're still nearby, waiting for you to do something incriminating."

"Threat #2 -- Same-day response anywhere in North America means surveillance might begin before you're ready. The FBI may end up watching you trying to hide the very material that you're hoping to conceal from them."

"Threat #3 -- The FBI's strategy of managed aggression in surveillance operations can provoke you into losing your temper or your nerve -- or both. It's a wicked mind-game. That's why they use it."

According to Adams, anyone can learn countersurveillance skills that make it difficult for the FBI to build a legitimate case against them.

"Perhaps even more important, they can make it difficult for the FBI to build a phony case against them," he says.

Adams says he has no plans to discontinue publishing his disclosures at his Web site at http://www.SPYCOUNTERSPY.com

---

The following news release was distributed February 17-18, 1998 by fax and email to 64 news media organizations and journalists in the USA, Canada, and UK.

News Release

For Immediate Release

Hacker divulges secrets of world's spy agencies.
CIA, FBI ops and foreign policy affected.

VICTORIA BC, CANADA – February 18, 1998 – A spy watcher in Canada is using the Internet to reveal the operating methods of the world's spy agencies. Lee Adams says he is breaking no laws by telling what he learned by watching the spies who were watching him.

"I'm just a hacker," admits Adams. "But I don't hack computer systems, I hack surveillance operations. I go after intelligence agencies and undercover cops."

Adams first came to the attention of the US intelligence community eight years ago during a routine vetting by a defense research facility to renew his clearance. Using skills he had learned while writing computer programming books for McGraw-Hill, he became adept at spotting the spies. When he took his concerns to the authorities, he was rebuffed – but the surveillance intensified.

Adams claims he found himself in the role of crash-test dummy as the spies attempted to upgrade their tradecraft. But while they were watching him, he was watching them.

"They were inadvertently showing me their best stuff," claims Adams. "So I provoked other groups into watching me. I wanted to learn as much as I could."

Adams claims that the United States has fallen 20 years behind the methods being used by other nations.

"Nowhere is this more evident than Iraq. The CIA has no

productive agents inside the country. Iraqi counterintelligence has neutralized them all," claims Adams. "US spy satellites and electronic eavesdropping can't find hidden weapons. To do that you need infiltration by human agents. And the US doesn't have any. That's why random bombing is the only option left."

"While the US was spending billions on high-tech surveillance gadgets, other countries were developing low-cost, low-tech solutions," says Adams. "These other groups now have a 20-year lead in humint, which is spytalk for human skills in surveillance and intelligence work."

Adams says he has no plans to discontinue publishing his disclosures at his Web site located at http://www.SPYCOUNTERSPY.com

---

The following news release was distributed February 11th, 1998 by fax and email to 59 news media organizations and journalists in the USA, Canada, and UK.

News Release

For Immediate Release

Spy watcher threatens to expose surveillance operations of FBI, CIA, and others on February 14th

VICTORIA BC, CANADA – February 11, 1998 – A spy watcher in Canada is threatening to use the Internet to expose dozens of active surveillance operations across the United States on February 14th. His action puts in jeopardy a number of operations in U.S. cities by the FBI, ATF, DEA, and local law enforcement agencies. Operations by the CIA outside the U.S. may also be affected.

Lee Adams says he will publish a simple three-step method that anyone can use to recognize surveillance teams operating in public locations.

Adams claims exposure of surveillance teams is inevitable because the U.S. has fallen twenty years behind the methods being used in other nations. He says the situation is a result of tunnel vision of U.S. bureaucrats and politicians.

"The United States spent the last two decades throwing billions of dollars at high-tech surveillance gadgets. During that same period, however, others have been developing low-cost, low-tech solutions," says Adams. "These other groups, not all of them friendly, now have a twenty-year lead in humint, which is spytalk for human skills in surveillance and intelligence work."

Adams says he will publish his three-step detection method at his Web site at www.SPYCOUNTERSPY.com two days prior to February 14th, in order to give authorities time to protect their most sensitive surveillance operations.

"If they leave those surveillance teams in place, they will be detected by anyone who chooses to try this simple three-step method," warns Adams. "The Web site says it all. How to catch your first spy this weekend."

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com
EMAIL ENCRYPTION: Return to main page. Click on *Ask Agent X* for public key.

Glossary

Updated October 9th, 1998

Words and phrases used by intelligence agencies, security services, law enforcement, resistance movements, guerrilla groups, and other underground organizations.

ACCESS AGENT – a talent spotter, performs reconnaissance for recruiters.
ACORN – slang for someone who is performing an intelligence function.
ACTION DIRECTE – an underground group in France.
AGENT – a person under the control of an intelligence agency or security service.
AGENT-OF-INFLUENCE – a deep-cover agent with influence among the members of a target group.
AGENT PROVOCATEUR – a deep-cover agent who feigns enthusiastic support while tempting the target to incriminate himself/herself through action or words .
AIS – Argentina's intelligence agency.
AL AMN AL-KHAS – Iraq's security service.
AMAN – one of Israel's intelligence agencies.
AMERIKA – underground metaphor for a fascist USA remeniscent of Nazi Germany.
ANALYSIS – drawing conclusions about raw information by assessing its significance and by collating it with other information.
ASALA – underground group in Armenia.
ASIO – Australian Security Intelligence Organization.
ASIS – Australian Secret Intelligence Service, a department of ASIO.
ASSAULTER – a member of a SWAT team responsible for making a forced entry.
ASSET – an agent.
AUM SHRINKYO – underground group in Japan with expertise in germ and chemical warfaire.
AVB – Hungary's security service, the Allami Vedelmi Batosag.
BACKSTOP – an arrangement between two persons for the express purpose of substantiating a cover story or alibi.
BAG JOB – surreptitious entry, break and enter.
BAKIN – Indonesia's security service.
BATF – a US security service, the Bureau of Alcohol, Tobacco, and Firearms.
BETTY BUREAU – FBI slang for a female support person who has worked for the FBI her entire career.
BfV – Germany's security service, the Bundesamt fir Verfassungsschutz.
BIOGRAPHICAL LEVERAGE – blackmail info.
BLACK-FLAGGED – an agent or intelligence officer who is to be interrogated and summarily shot if apprehended.
BLIND DATE – the first meeting with an unknown person.
BLACK PROPOGANDA – a smear campaign, usually consisting of character assassination.
BLOWBACK – unexpected negative consequences of spying activity.
BLOWFISH – a mathematical algorithm for computer encryption of text that purportedly can only be cracked by brute force if the passphrase is unknown.
BLOWN – detected.
BLUE-ON-BLUE – friendly fire, inadvertent hostile engagement between allies.
BND – Germany's intelligence agency, the Bundesnachrichtendienst. Literally translated as the Federal News Agency.
BOX – slang for Britain's security service, MI.5.
BREVITY CODES – a system of code-words used by members of a surveillance team.
BRICK AGENT – an FBI agent who works inside a field office. Also see STREET AGENT.
BRUSH CONTACT – a clandestine, momentary contact

between two agents who are passing information, documents, or equipment.
BRUSH PASS – same as brush contact.
BSS – Belgium's security service
BUCAR – an FBI car.
BUG-ON-A-CHIP – slang for USA's Clipper chip.
BUPO – Switzerland's security service.
BURNT – burned, completed exposed. See BLOWN.
BVD – Netherlands' security service.
CALL-UP – a police term meaning a situation where a SWAT team has deployed.
CANNON – a thief who steals back the inducement offered by the spies to an informant, defector, etc.
CARIBINIERI – Italy's federal antiterrorist police.
CASE OFFICER – operations officer, controller.
CBI – India's security service.
CHASE CAR – a security detail or bodyguard vehicle that follows the subject.
CHEATING – command of the target from *in front of* the target during floating box surveillance. See also COMMAND OF THE TARGET.
CHENG PAO K'O – China's intelligence agency.
CHICKEN FEED – low grade information fed through a double agent to one's adversary with the intention of building the credibility of the double agent.
CHOBETSU – One of Japan's security services.
CIA – a US intelligence agency.
CNT – an acronym for crisis negotiation team. CNTs are used by police in situations involving hostage-takers or barricaded suspects. The name CNT is a misnomer – their true role is not to negotiate, but rather to obtain intelligence to facilitate an assault by the SWAT team, and to distract the suspect to divert his attention from the coming assault.
COMINT – acronym for communications intelligence.
COMM – a small note or other written communication from an underground organization or one of its members. They are typically written on cigarette wrappers, chewing gum wrappers, etc.
COMMAND OF THE TARGET – active visual observation of the subject of the surveillance operation. Used during pedestrian and vehicle surveillance. See also CHEATING and FLOATING BOX.
COMMANDO – a civilian, military, or paramilitary combat group using irregular tactics. Commando can refer to an individual, a cell, a squad, or the organization as a whole.
COMMIT – a surveillance operative performing the commit function is watching a location to determine the direction that the target takes (or "commits" to).
COMPROMISED – breached security status.
CONG AN BO – Vietnam's security service.
CONSUMER – a person or an organization on an intelligence agency's distribution list. Also see PRODUCT.
COOKED – a mixture of genuine and fake material provided via a double agent to one's adversary.
COORDINATION DE LA SECURITE DU TERRITOIRE – Algeria's security service.
COUNTERESPIONAGE – activities designed to impede the efforts of hostile intelligence agencies engaged in espionage against one's own nation, allies, and citizens.
COUNTERINTELLIGENCE – activities designed to impede or thwart the efforts of hostile intelligence agencies attempting to penetrate or compromise one's own intelligence agency.
COUSINS – slang for CIA.
COVER – persona, profession, purpose, activity, fictitious image maintained by an undercover operative.
COVERT ACTION AGENT – a spy who works to reorient an entire nation's politics in favor of his country.
CS GAS – a form of tear gas, full name ortho-chlorobenzalmalanonitrile, used by cops, SWAT teams, and the military.
CSE – Canada's sigint intelligence agency, Communications Security Establishment. http://www.cse.dnd.ca/
CSIS – Canada's security service.
CUT-OUT – a go-between used to preserve the safety or

anonymity of the principals. Same as LETTERBOX.
COURIER – delivers documents, money, etc.
DAM – France's military intelligence agency.
DANGLE – a spy who poses as a walk-in to penetrate the other side. Also see WALK-IN.
DARPA – Defense Advanced Research Projects Agency (USA).
DATA RECOVERY – bureaucrat-talk for the backdoor built into *all* US-exported crypto software since 1998.
DCSS – Denmark's security service.
DDIS – Denmark's intelligence agency.
DEAD DROP – a physical location where communications, documents, or equipment is covertly placed for another person to collect without direct contact between the parties.
DEAD-LETTER BOX – same as dead drop.
DEAD-LETTER DROP – same as dead drop.
DECOY – distracts adversary's attention.
DEEP-COVER AGENT – permanent cover.
DEFECTOR – a person who has renounced his/her country of citizenship.
DGI – Cuba's intelligence agency.
DGSE – France's intelligence agency.
DIA – a US intelligence agency, the Defense Intelligence Agency.
DIRTY TRICKS – covert sabotage carried out by a security service or intelligence agency, ranging from pranks to assassination.
DIVERSION – distracts adversary's attention.
DLB – acronym for dead-letter box. Also see DEAD DROP.
DOPE BOOK – a notebook kept with a sniper rifle for the purposes of recording the atmospheric conditions, range, lighting, and resulting hit or miss of every shot fired.
DOPPELGANGER – a lookalike. See also LOOKALIKE.
DOUBLE-AGENT – simultaneously serves two adversaries (often with their knowledge).
DRY CLEANING – active countersurveillance and antisurveillance against pavement artists and wheel artists.
DS – Bulgaria's security service, the Drzaven Sigurmost.
DSD – Australia's sigint agency, Defence Signals Directorate. http://www.dsd.gov.au/
DST – France's security service.
DUBOK – Russian term for a dead-letter box. Also see DEAD DROP.
E&E – escape and evasion.
ELEMENT – a five-man SWAT team. Consisting of a team leader, scout, rear guard, and two assaulters. The rear guard provides cover for the scout and is usually armed with a 12-guage shotgun. The assaulters usually carry Heckler & Koch 9mm MP-5 submachine guns. See also ASSAULTER.
ELLIPTICAL CONVERSATION – says one thing but means another.
EQUESTRIAN POSTURE – an effect produced by *rigor mortis* whereby the cadaver sits upright as if riding in a saddle, with arms outstretched.
ESPIONAGE – clandestine collection of intelligence by a non-domestic intelligence agency.
ESS – acronym for environmentally stable strategy, a concept used in strategic game-theory.
ETA – an underground group in Spain.
EVOC – an acronym for Emergency Vehicle Operation Course, taught at the FBI academy in Quantico.
FALN – an underground group in Puerto Rico.
FALSE FLAG RECRUITMENT – impersonation by a spy while recruiting an informant, defector, agent, etc.
FBI – a US security service.
FDS – One of Mexico's security services.
FIBONACCI SYSTEM – a system of non-carrying addition used for one-time pad codes. For example, (Fib) 999 + 222 = 111.
FILLING – the act of inserting material in a dead drop.
FLIP – a U Turn made by the target during a vehicle surveillance operation.
FLOATING BOX – a method of surveillance where a team of operators establishes a containment box around the target wherever he/she goes.
FMLN – [illegible]

FMLN – Frente Farabundo Marti para Liberacion Nacional, an underground group in El Salvador.
FOLLOW – a surveillance team is executing a follow when they are shadowing a moving target. See also FLOATING BOX. A follow begins when the target exits the stakeout box and a surveillance operative attains command of the target. See also COMMAND OF THE TARGET.
FOOTFALL DETECTOR – vibration sensor designed to detect walking humans.
FOUR-BAGGER – disclipline of an agent by FBI headquarters, consisting of censure, transfer, suspension, and probation.
FRA – Sweden's military signals intelligence agency.
FREQUENCY FLOODING – a technique that allows an ordinary telephone to become a covert listening device.
FRIEND – slang for an agent, informant, or mole providing information to a handler.
FRIENDS – slang for Britain's secret intelligence service, MI.6.
FRONT – a legitimate-appearing business created by an intelligence agency or security service to provide cover for spies and their operations.
FSB – Russia's federal security service, responsible for counterespionage.
FUNKSPIEL – impersonation during electronic communications. Derived from the German phrase for "radio game".
FUNNY PAPER – slang for the counterfeiting and forged documents section of an intelligence agency or security service.
GCHQ – Britain's sigint agency, Government Communications Head Quarters. http://www.gchq.gov.uk
GIA – an underground group in Algeria.
GID – Iraq's main intelligence organization, Da' Irat al Mukhabarat al-Amah.
GRU – Russian military intelligence, the Glavnoye Razvedyvatelnoye Upravleniye.
GSS – Israel's security service (also called Shin Beth).
GUAN-XI – an access agent for China's intelligence agency
GUOANBU – one of China's security services.
GUSTAV WEBER – Hitler's double, used by the Fuhrer's bodyguards to stymie the Allies as to his whereabouts. Shot in the forehead immediately after Hitler's death.
HAMAS – an underground group in Palestine.
HARD MAN – an experienced operative who can survive in a hostile environment and who has killed.
HARD TARGET – a surveillance target who is actively maintaining secrecy and may not reveal that he/she has detected the surveillance team.
HEZBOLLAH – an underground group in Lebanon, alleged to have operating units in Latin America with links to major drug dealers.
HONEY POT – Mata Hari, Raven, lady, femme fatale; a female agent using romance to compromise a target.
HOOLIGAN TOOL – a specialized tool much like a crowbar, developed by fire departments for prying open doors and windows. Also used by SWAT teams.
HOSTILE RECRUITMENT – recruitment by threat or force of an uncooperative informant, mole, or agent-in-place.
HUMINT – intelligence activities involving people rather than electronic eavesdropping or communications interception.
HUNTING PACK – slang for surveillance team.
IAKHBAL – Israeli police unit that fights organized crime.
ICBM – an acronym for instant calm breath method, a way to overcome the flight-or-fight reflex (panic). Also reduces hyperventilation.
ILD – one of China's security services.
ILLEGAL – an intelligence officer operating in a foreign nation without the protection of diplomatic immunity.
IMINT – acronym for image intelligence.
INFORMANT – a legitimate member of a target group providing intelligence to the surveillance team.
INTELLIGENCE OFFICER – a trained member of an intelligence agency, an employee on salary.
INTERPOL – international police body that coordinates the intelligence gathering and investigative activities of member police forces.
INVESTIGATIVE SPECIALIST – the FBI's name for a

INVESTIGATIVE SPECIALIST – the FBI's name for a surveillance operative (vehicle or foot). Pay grade GS-7 to GS-10. See also SSG.
IRA – an underground group in Northern Ireland.
ISTIKHBARAT AL ASKARIYA – Libyan military intelligence.
ITAC – an acronym for International Terrorist Assessment Center, located in Washington DC.
JARKING – bugging a weapons cache, often rendering weapons unusable.
JETRO -- one of Japan's intelligence agencies.
JIHAZ AMN AL DAOULA – Egypt's security service.
JOE – a deep-cover agent.
JRA – Japanese Red Army, an underground group in Japan.
KEMPEI TAI – Japan's secret police.
KGB – Kometet Gosudarstvennoi Bezopasnosti.
K-LINE – SVR internal security and investigations section.
KOANCHO – Japan's counterintelligence and security service.
L5 – 4096 bit encryption algorithm
LADY – honey pot.
LAKAM – one of Israel's intelligence agencies (Ministry of Defense).
LEGEND – the faked biography of a deep-cover agent.
LETTERBOX – a person who is acting as a go-between. Also see CUT-OUT.
LINK DIAGRAM – connections being analyzed in a complex police investigation or counterespionage case. See problem-solving matrix.
LLB – an acronym for live-letter box, an address used to receive communication to be forwarded to an intelligence agency. See also DLB.
LOOKALIKES – decoys used to confuse hit squads and surveillance teams.
LSD – an acronym for d-lysergic acid diethylanide, a hallucinatory drug discovered in 1943 by Dr. Albert Hofmann, a researcher at Switzerland's Sandoz corporation, a pharmaceutical manufacturer. Subsequently monopolized by the CIA for its MKULTRA project that developed methods for secretly controlling people. Still used today by numerous intelligence agencies and security services for the following functions – 1. disturbance of memory; 2. discrediting by aberrant behavior; 3. eliciting of information; 4. creation of dependence; 5. suggestibility. At the CIA's request, in 1954 Eli Lilly & Company developed a method for manufacturing LSD from publicly available chemicals. The CIA's bungling of MKULTRA allowed the drug to escape from the lab, where the CIA lost control of it. LSD subsequently ruined two generations of young Americans. No CIA officer or contractor was ever reprimanded or punished.
M-19 – underground group in Columbia.
MASKIROVDA – Russian name for deception techniques designed to fool US spy satellites. Recently used by India's counterintelligence agency to conceal nuclear testing from the CIA.
MATA HARI – honeypot, femme fatale,
MBRF – one of Russia's intelligence agencies.
MERCURY FULMINATE – an initiating agent for detonating PETN. See PETN.
MI.5 – Britain's security service. K Branch is responsible for counterespionage, F Branch for countersubversion, C Branch for security of sensitive government installations.
MI.6 – Britain's intelligence agency.
MICE – an acronym for money ideology compromise ego (methods used by intelligence agencies and security services to ruin a target).
MINI MANUAL OF THE URBAN GUERRILLA – an underground operations manual by Brazilian freedom-fighter Carlos Marighella. Contains 41 chapters. Banned in many countries.
MIN/MAX – a concept in strategic game-theory.
MITI -- one of Japan's intelligence agencies.
MOLE – a penetration agent.
MONTENEROS – an underground group in Argentina.
MOSSAD – one of Israel's intelligence agencies, noted for its expertise in wet affairs. Literally translated as "institute". Never referred to as *the* MOSSAD, but rather simply called MOSSAD.
MST – Landless Rural Workers Movement, an underground

group in Brazil.
MUKHABARAT – Libya's intelligence agency.
MUSLIM UIGHUR – an underground group in China.
NAICHO – one of Japan's intelligence agencies.
NARCOTHERAPY HYPNOSIS – CIA interrogators use hypnosis to force regression in the prisoner to make him believe he is talking to his spouse. The prisoner is first prepared by pharmaceuticals according to the following protocol. 1. An injection of 10 mg sodium pentothal to render unconscious. 2. Wait 20 minutes. 3. An injection of 10 mg benzodrine to revive the prisoner to a state partway between waking and sleep. 4. Repeat step 3 if required. At the end of the interrogation a hypnotically induced amnesia is invoked.
NEUROLINGUISTICS – a branch of psychology used by intelligence agencies and security services to covertly manipulate unsuspecting human targets.
NEUTRON BOMBARDMENT – used by security services like Britain's MI.5, America's FBI, Germany's BfV, and France's DST to detect microdots and invisible writing in postal mail. Originally developed by the Atomic Weapons Research Establishment in Britain for use by MI.5.
NIGHTCRAWLER – a talent spotter who prowls bars and nightclubs looking for government employees, military personnel, etc. who can be compromised using booze, drugs, or sex. Also see TALENT SPOTTER.
NINJAS – slang for members of a SWAT team.
NITROUS OXIDE – an anesthetic inhalant used to render sleeping targets unconscious during surreptitious entry by goon squads.
NMI – Norway's security service.
NPA – National Peoples' Army, an underground group in the Philippines.
NSA – US sigint intelligence agency and security service, the National Security Agency. http://www.nsa.gov:8080/
NSS – Bulgaria's security service.
NSTL – the FBI's national security threat list.
OBS – Croatia's intelligence agency, the Obavestajna Bezbednostna Sluzba.
OP – observation post.
OFFENSIVE PENETRATION OPERATION – infiltration of an agent into a target group or organization.
OFFSITE – a covert FBI site or facility situated away from a field office.
OG – an acronym for original gangmembers, now in their thirties and forties, who supply cocaine and heroin to street gangs.
ONE-TIME PAD – an unbreakable code system that works by adding the numeric value of the plaintext with a randomly-generated code string (the one-time pad). Also see FIBONACCI SYSTEM.
OSA – official secrets act, usually a law to enable governments to conceal their mistakes from their own population.
OUTRIDER – a wheel artist responsible for ensuring that the target does not get outside the floating box of surveillance vehicles. See also FLOATING BOX.
OVERT TARGET – deliberately attempts to draw attention and drain the resources of an intelligence agency or security service. Occasionally a decoy.
PARALLEL-LINE/INCIDENTAL-CAPACITANCE – a method of telephone, telex, and communications eavesdropping that is virtually undetectable.
PAVEMENT ARTIST – outdoor surveillance specialist operating on foot.
PEEP – photographer.
PERIMETER SURVEILLANCE – is used to alert the surveillance team when the target enters or leaves a specific area.
PETN – Pentaery-thritol tetranitrate, a plastic explosive favored by intelligence agencies and security services. See mercury fulminate.
PFLP – an underground group in Palestine.
PHOTINT – acronym for photo intelligence.
PICKET SURVEILLANCE – focuses on times and places when target is likely engaged in activities of interest to the surveillance team. Also called chokepoint surveillance. Named

after the openings in a picket fence.
PICKUP – when the target of a surveillance operation is first spotted inside the stakeout box.
PINHOLE CAMERA – video camera with fiber-optic lens attachment.
POSSE COMITATAS – a Latin phrase that loosely means *power of the people*.
PROBLEM-SOLVING MATRIX – a grid-based notation system used by police investigators and counterespionage officers when dealing with complex cases.
PRODUCT – finished intelligence that has been evaluated by an intelligence agency and is ready for distribution to consumers. Also see CONSUMER.
PROFESSIONAL-NAME – nom de guerre of a spy.
PROFILE STOP – a random stop and search by police, based on a suspect's race, minority status, economic status, religion, physical appearance, travel status, location, etc. Previously inflicted on minorities and poor whites, but currently being expanded by bureaucrats to include all US citizens.
PSB – one of China's secret police agencies.
PSIA – one of Japan's security services.
PSYCHIC COMBAT – a condition of active psychological warfare operations between two covert adversaries.
PSYCHODYNAMICS – the CIA's psychological profiling system, used in combination with psychobiographic analysis.
QUANG BO – Vietnam's military intelligence agency.
QODS – One of Iran's security services.
QRF – quick reaction force.
RADINT – acronym for radar intelligence.
RAID – an acronym for Rapid Assessment and Initial Detection, consisting of teams of National Guardsmen who assist civilian authorities after a suspected biological/toxin/chemical attack on a population center.
RAVEN – a honey pot.
RCMP – police agency in Canada similar to the FBI in the USA. Acronym for Royal Canadian Mounted Police. Also known as RCM Police.
RCMP SECURITY SERVICE – counterespionage, counterintelligence, and counterterrorist branch of RCMP. Also known as RCMP SPECIAL SERVICES.
RED BRIGADE – an underground group in Italy.
RENT-A-GOONS – operatives proficient in hand-to-hand combat, used as muscle support when direct physical confrontation is likely.
RESISTANCE – a civilian underground organization, consisting of cells (1 to 10 persons), circles (a group of cells), and sections (a group of circles).
RG – France's police intelligence security service, Renseignements Generaux.
RING – a network of spies or agents.
ROSCOE – handgun.
RUSE DE GUERRE – subterfuge.
RZ – an underground group in Germany. Literally translated as revolutionary cells.
SA – FBI special agent.
SAFEHOUSE – a dwelling place or hideout unknown to the adversary.
SAPO – Sweden's security service.
SASHA KVAP – Russian mole inside Hitler's bunker during the final months of World War II. Subsequently poisoned by the KGB in 1955.
SAVAK – one of Iraq's security services.
SCIF – acronym for Secured Compartmentalized Information Facility (in Fort Gillem, GA, USA) where Clipper is housed (rumored to have already been penetrated by agents of China's intelligence agencies).
SEMTEX – a military explosive suitable for sabotage and terrorist operations.
SECRET CLASSIFICATIONS – Confidential, Secret, Top Secret, and (SCI) Special Compartmentalized Information.
SERE – an acronym for survival, evasion, resistance, and escape.
SERVICING – the act of removing material from a dead drop.
SET UP – to begin to conduct surveillance on a target.

SEVENTY-ONE YARDS – according to FBI statistics, this is the distance at which a typical police sniper will get you. Although the SR60 .308 sniper rifle used by most police departments is designed for distances up to 600 yards, most police snipers do not fire at suspects beyond 400 yards. (Of course, at any distance an *execution* is still an execution.)
SHIN BETH – Israel's security service (also called GSS).
SHINING PATH – an underground group in Peru.
SMERSH – KGB assassination group. Officially disbanded ;) The name derives from the Russian phrase "death to spies".
SIDE – Argentina's security service.
SIGINT – signals intelligence (interception of electronic communications)
SINN FEIN – the political arm (party) of the IRA.
SIS – one of Britain's intelligence agencies, the secret intelligence service.
SIT REP – situation report.
SIX – slang for a police officer, police cruiser, or a police patrol. Used as a warning in the criminal community.
SLEEPER AGENT – an inactive deep-cover agent.
SLUZBA BEZPIECZENSTWA – Poland's security service, also called the SB.
SOFT TARGET – an easy surveillance target, untrained and not looking for surveillance.
SOG – an acronym for Special Operations Group, FBI agents who conduct surveillance. In contrast, SSG is composed of non-agents. See also SSG.
SOS – dot dot dot dash dash dash dot dot dot.
SPECIAL BRANCH – the security branch of the British police.
SPLASHED – describes a bodyguard whose client has been assassinated. Also see WET AFFAIR.
SPOOK – a spy.
SPY – any member of an intelligence agency, security service, police agency, resistance movement, guerrilla group, or other organization engaged in covert intelligence-gathering activities.
SRI – Romania's security service (rumored to be made up of former members of Ceausescu's secret police).
SSG – an acronym for Surveillance Specialist Group, which is what the FBI calls a surveillance team. See also INVESTIGATIVE SPECIALIST. See also SOG.
SSS – Georgia's security service.
StB – Czechoslovakia's security service, the Statni Tajna Bezpecnost.
STINGBALL – a flashbang grenade used by SWAT teams to disperse crowds and disorient barricaded suspects. Throws off rubber fragments when detonated. It is standard police procedure to cover up the deaths of suspects inadvertently killed by stingballs.
STREET AGENT – an FBI agent whose work takes him to various locations. Also see BRICK AGENT.
SVR – one of Russia's intelligence agencies, the Slnzhba Vneshnei Razvedaki.
SWARMING – overfilling a location with surveillance operatives. Often used in psy ops as a means for controlling the target's environment.
SYNTHETIC HEMOGLOBIN – a component used in carbon monoxoide detector alarms. The radiation weapons recently developed and deployed by DARPA will set off these alarms.
TALEBAN – underground group in Afghanistan.
TALENT SPOTTER – same as ACCESS AGENT.
TARGET – the victim of surveillance, the subject.
THERMAL IMAGER – a heat-sensitive surveillance video camera and display.
THREE Bs – Booze, broads, and bucars. The three temptations of FBI agents. (If the choice of words offends our women readers, please remember that this is a phrase originated and used by FBI agents. We are merely reporting it.)
THROW PHONE – a cellular telephone thrown to a barricaded suspect by the SWAT team.
TRIADS – Asian organized crime gangs.
TRIGGER – a surveillance operative who is watching the target's vacant vehicle, home, garage, office, restaurant etc. and who alerts the rest of the surveillance team when the target is spotted.
TUPAMAROS [illegible]

TUPAMAROS – an underground group in Uruguay.
UACB – FBI acronym for Unless Advised to the Contrary by the Bureau.
UNITED RED ARMY – an underground group in Japan.
UNS – Croatia's security service, the Ured za Nacionalnu Sigurnost.
UNSUB – an unknown subject in a surveillance operation.
UOP – Poland's security service.
USSA – slang for a USA reminiscent of the oppressive totalitarianism of the former USSR.
VCP – vehicle control point.
VEVAK – Iran's intelligence agency.
VICKIE WEAVER – American citizen probably murdered by the FBI. A landmark case for many concerned Americans.
WAHABI – a Saudi Islamic underground group .
WALK-IN – an unsolicited volunteer.
WATCH-LIST – people targeted for routine surveillance.
WET AFFAIR – results in death of target. Also see SPLASHED.
WHEEL ARTIST – an outdoor surveillance specialist operating in a vehicle.
WILDERNESS OF MIRRORS – a spy operation so complicated that it is no longer possible to separate truth and untruth.
X RAYS – used by intelligence agencies and security services to pick key-locks and to deduce the settings for combination locks. Equipment fits in a standard briefcase.
ZAPATISTA NATIONAL LIBERATION ARMY – an underground group in Mexico.
ZERO-OUT – the range at which a weapon's sights will produce a bull's eye hit. Handgun fixed sights are usually zeroed-out at 25 yards. A sniper rifle scope is usually zeroed-out at 100 yards. The term *cold barrel zero* refers to the calibration of a SWAT sniper rifle so that the first (cold) shot will hit a target at 100 yards. Subsequent rounds will diverge due to barrel heating.
ZHONGYANG LIANLUOBU – one of China's intelligence agencies.
ZOU-HOU-MAN – back door access to a protected target (as used by China's intelligence agencies).

Back to Home Page

OFFICE: 3273 Tennyson Avenue, Victoria, British Columbia, Canada.
MAIL: PO Box 8026, Victoria BC, CANADA V8W 3R7.
TELEPHONE: (250) 475-1450.
FAX: (250) 475-1460.
EMAIL: reader_service@SPYCOUNTERSPY.com