"Spy school for the rest of us."

This PDF version of the now defunct Spy & CounterSpy website (including all extant issues of the F9 bulletin) has been slightly altered: Some redundant material been elided, and a scant few annotations added. Carlos Marighella's *Mini-Manual of the Urban Guerrilla* is included in full as an appendix.

Send comments/questions to:

Phosphor <phosphor@redirect.to>
Find my public key at:
http://redirect.to/phosphor

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*

...

Contents

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.

...

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

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 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

Learning the basics...

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.

...

...

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

What's really happening here...

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.

...

...

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

Wake-up call...

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.

...

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.

...

...

...

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.

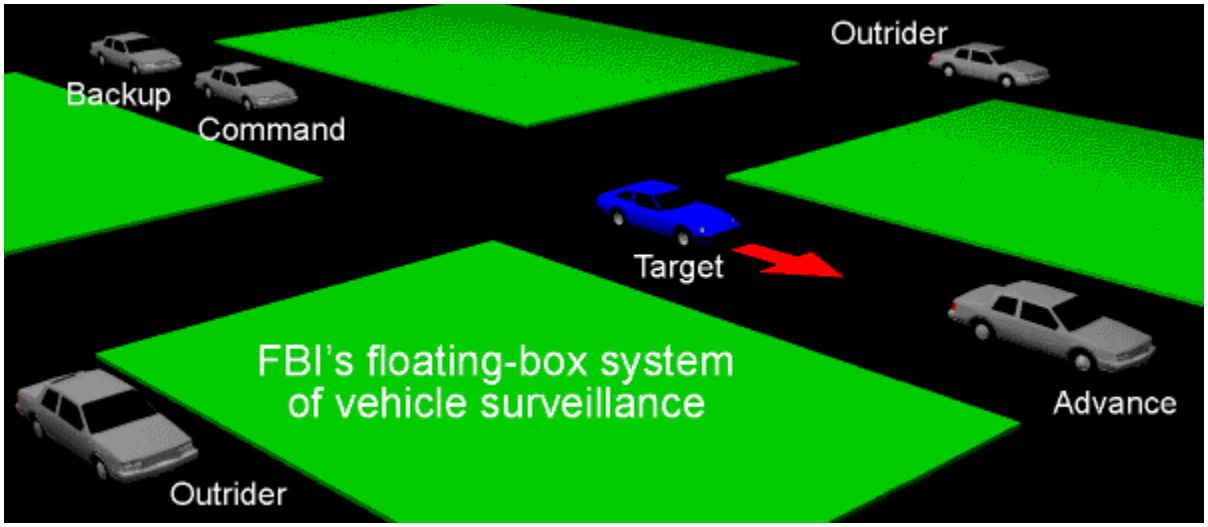
The FBI's floating box system...

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 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.

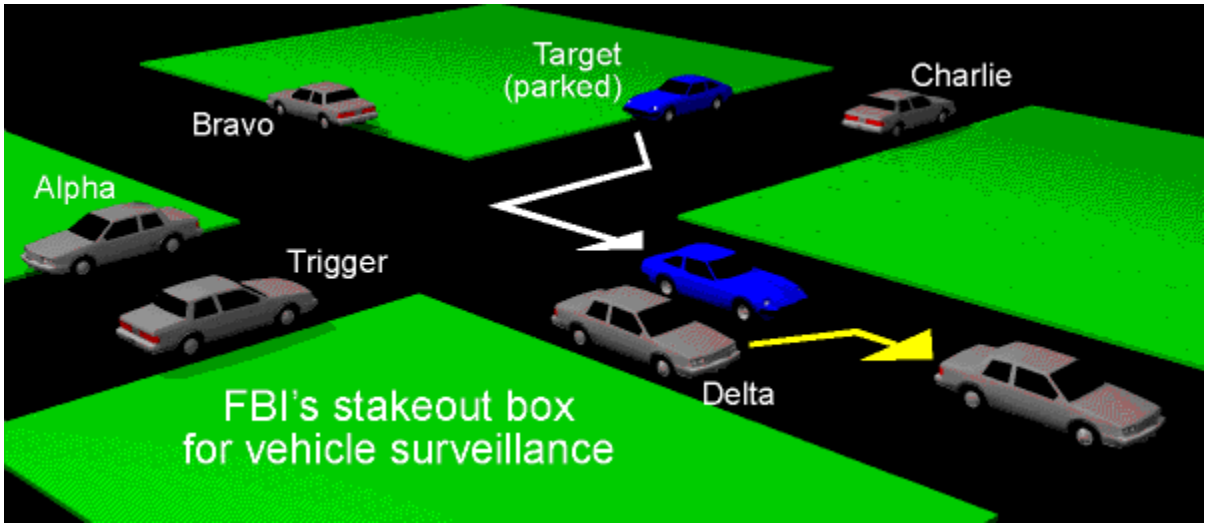
Signature shift. The floating-box makes it possible to quickly alter the signature of the team, making them more difficult to detect. In the previous illustration of the floating-box system, there are five surveillance vehicles. At first glance one might assume they can be reconfigured five different 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.

...

...

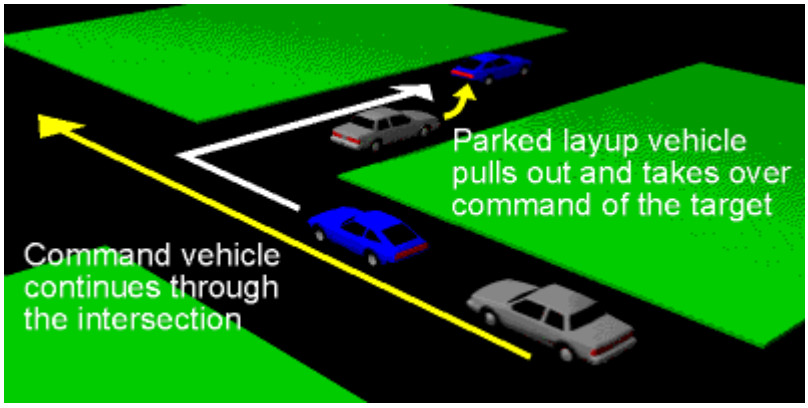
Command of the target...

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.

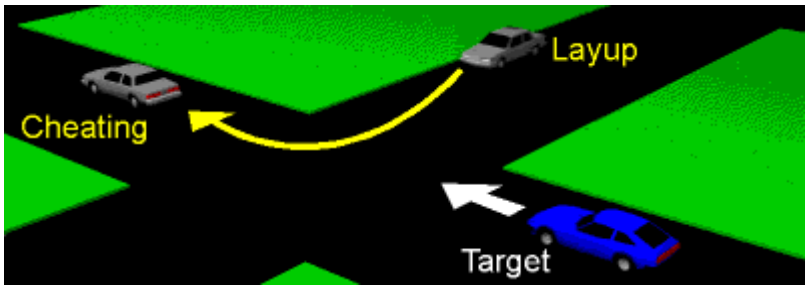


After watching the target make a right turn at the intersection, the *command vehicle* continues straight through the intersection. The agent has, however, alerted one of the *layup vehicles* that the FBI has prepositioned at major *decision points* along the target's route.

As you can see from the illustration above, this is a very

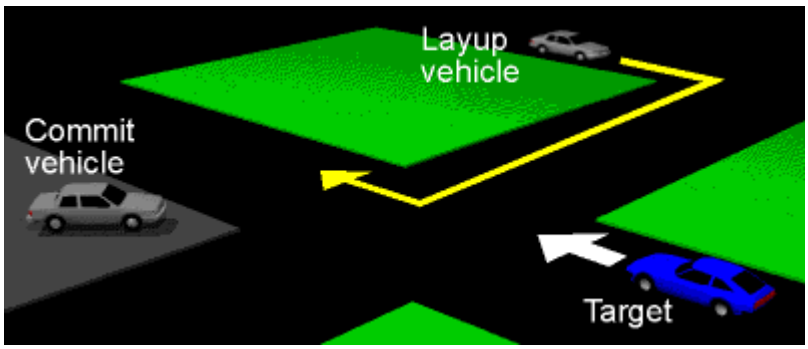
potent maneuver. The target sees the car that has been following him continue straight through the intersection. He starts to question whether or not he was actually under surveillance – perhaps he was just "imagining things". As a result, the *layup vehicle* is often able to pick up *the follow* without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

...

Content Warning – This article provides sensitive information to concerned citizens who want to resist government tyranny and repression. If you are a minor or a criminal, please leave now – and don't come back.

...

...

...

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.

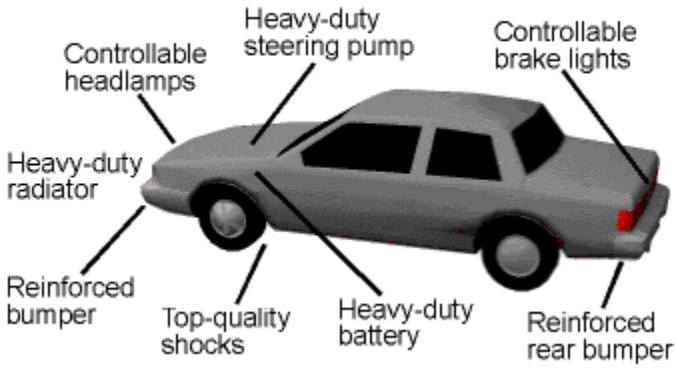
You'll also see how the members of the surveillance team communicate with each other. You'll learn why you never see them talking.

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, station wagons, 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.

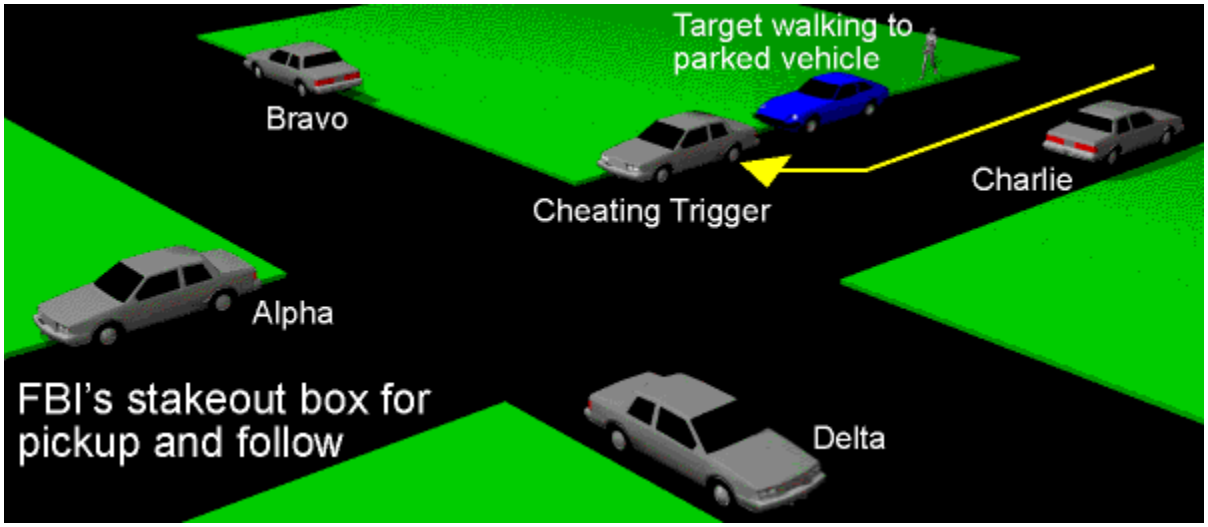
Wheel artist – numerous clicks.
Controller – "Is that you, Echo?"
Wheel artist – two clicks (*Yes*).
Controller – "Are you in command of the target?"
Wheel artist – two clicks (*Yes*).
Controller – "Has the target made contact with the other suspect yet?"

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*.

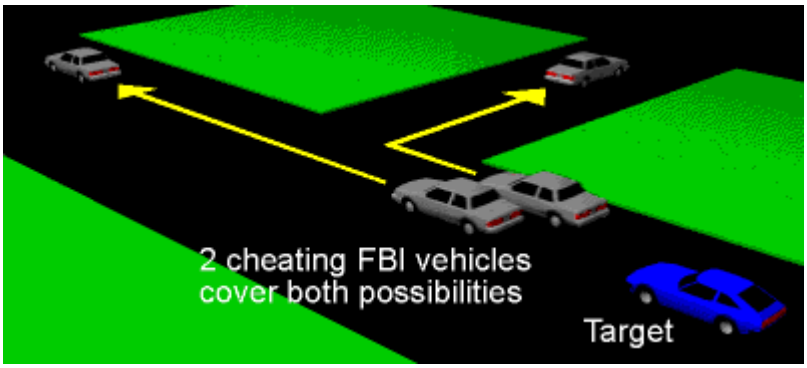
Fundamental tactics...

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.

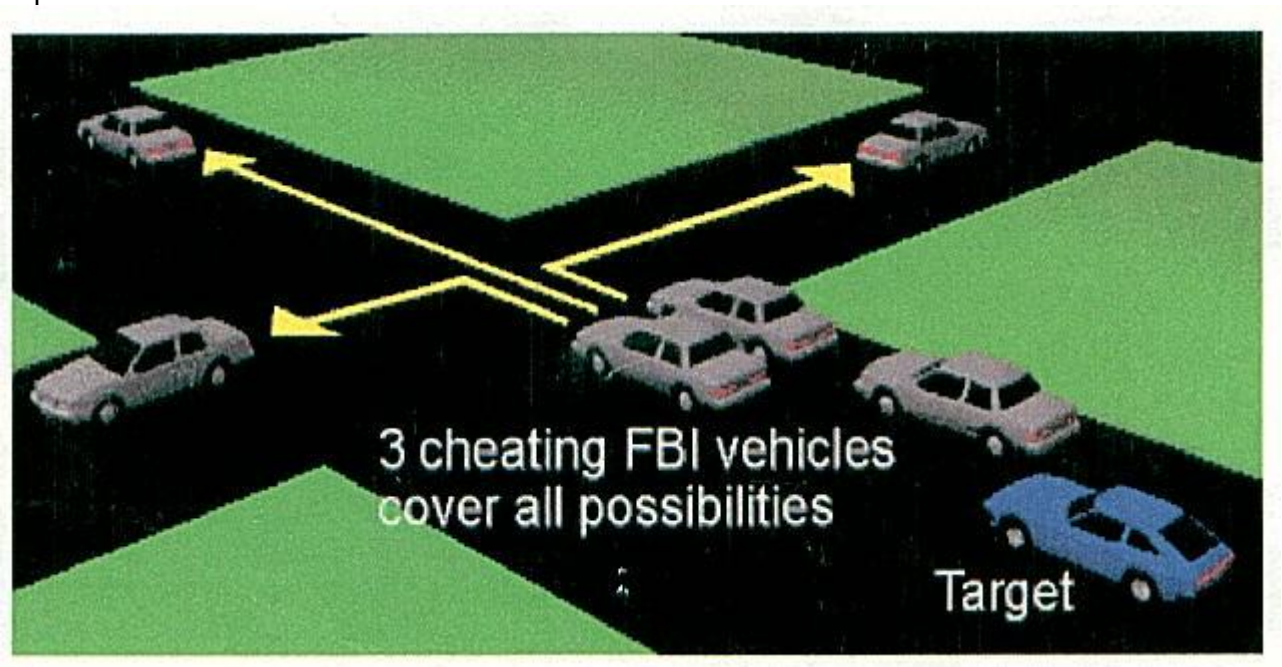


The cheating intersection. When the target is approaching a decision-point – and her direction of travel cannot be predicted by the FBI – the surveillance team leader makes certain that two FBI vehicles are in front of the target's vehicle. This is a deadly tactic. It has meant the ruin of many suspects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

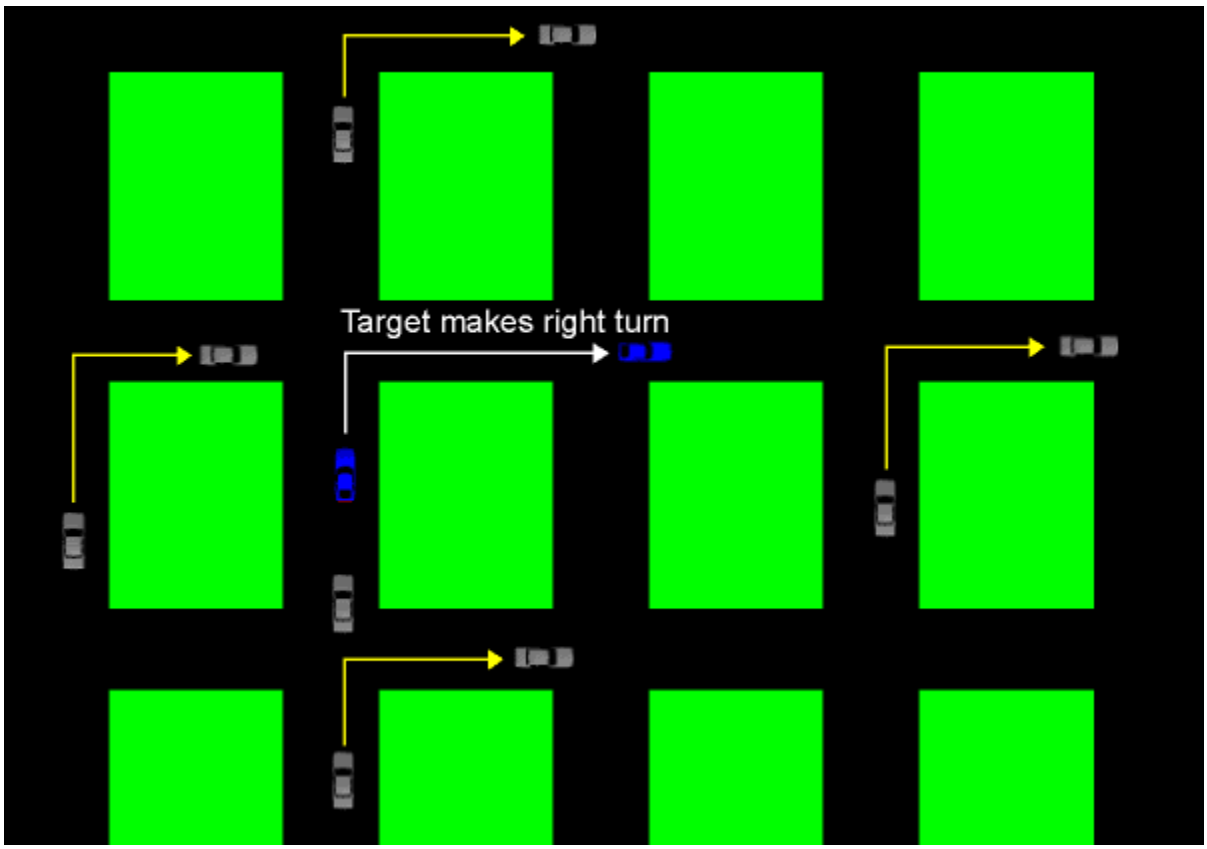
As shown in the illustration above, each *cheating* FBI vehicle takes a different route. The FBI has every possible scenario covered. No matter which route you choose, a *cheating* FBI surveillance vehicle (positioned in front of you) has you covered.

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.

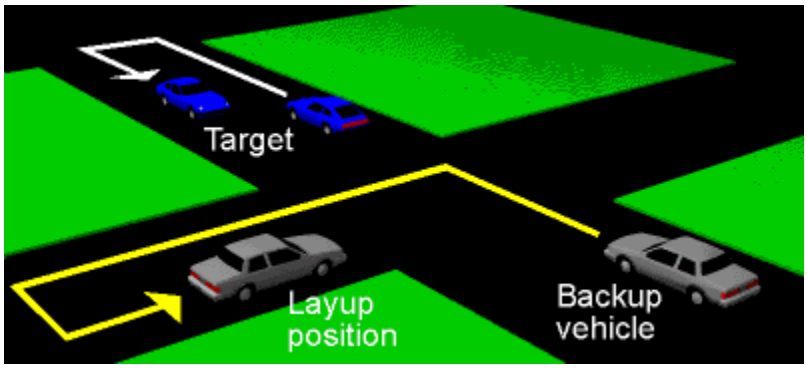
In the situation shown above, the former command vehicle usually continues straight through the intersection, so as not to attract attention to itself. It will be replaced by another FBI agent being held in reserve by the team leader.

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 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 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 & 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.

...

...

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

How surveillance is triggered...

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..

...

...

SPY & COUNTERSPY

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.

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.

...

...

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

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 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.

...

...

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

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.

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 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 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.

SPY & COUNTERSPY

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*.

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.

...

...

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

Protocol 1:
The firewall method...

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.

...

Protocol 2:
The deception method...

...

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 café can 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.

...

You can boost your chances of stopping an FBI surveillance team from learning anything at all.

Summary...

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 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.

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.

...

...

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

A question of control...

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...

...

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 andmeetings, 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.

...

...

This crisis has been about 30 years in the making.

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

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 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.

...

...

All this technology gives government tremendous power over us.

Privacy forbidden... New surveillance capabilities

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.

...

...

...

SPY & COUNTERSPY

How to organize a resistance movement...

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.

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.

SPY & COUNTERSPY

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 sécurité* – a French phrase which can be translated as *security run* or *security circuit*.

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 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

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

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.

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*.

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

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

How to broadcast to a group of cells...

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.

...

...

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 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...

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.

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

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

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.

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.

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

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-provocateur.

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.

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

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.

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.)

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

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

...

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. **;)**

...

...

...

...

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.

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

...

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.

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.

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.

...

...

...

...

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.

Lesson 2:
How to *pretend* you're not being fleeced by the government...

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

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.

the 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.)

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.

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.

...

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

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*.

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.

...

...

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

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*.

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.

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.

...

...

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*.

Episode 1: Reconnaissance – The FBI's Advance Team

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.

...

...

...

...

...

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.

Security software...

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. **[Now known as EnCase. Download it from a P2P network. - Phosphor]** 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.

[My own forensics tests with File Vault reveal that the wipe utility leaves the job only half-done, giving users a dangerous sense of false security. Parisien, the company that developed File Wipe, also works closely with government. See my own page for useful software and information: http://geocities.com/phosphor2013 - and feel free to mirror it, as it may soon be "disappeared". - Phosphor]

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.

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.

...

SPY & COUNTERSPY

About Agent X...

Agent X is not one agent, but *three*. Agent X 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.

You are being swindled.

Here is the big picture...

...

Simply stated, here is the reason why *Spy & CounterSpy* was created – to address a problem that confronts us all.

...

In brief...

The moneyed interests are taking the *best of everything* while they distract the rest of us.

...

The situation today...

Inequality, injustice, and instability are the norm for the *have-nots* like you and I. Meanwhile the wealthy and powerful wallow in a luxury that is *intentionally concealed* from the rest of us. Our attention is deliberately *diverted and distracted* by alcohol, drugs, sports, music, movies, and television. They pacify us with trivial diversions while they loot and plunder a planet that is beginning to show the early warning signs of ecosystem collapse.

...

The adversary...

Our invisible warder is the industrial regime and its enforcer, the nation-state. In practical terms that often means multinational corporations and their *directors*, *executives*, and *management*. It also means the *politicians* and *bureaucrats* who have betrayed our naiive trust and sold us out.

...

The reins of power...

Simply stated, the industrial regime *runs* the nation-states of the world. The industrial regime demands that *its* priorities dominate and *its* interests be defended – with "anticipatory retaliatory" cruise missile strikes if need be. With a *Desert Storm*, if push becomes shove.

BACKGROUND – Never before in human history has a government resorted to such *brutal measures* – coerced informants, illegal arrests, crooked judges, rigged trials, and a tethered news media. Force (often disguised) is used by the nation-state to ensure that moneyed interests are *free to do as they want*. This is the stark truth of laissez-faire.

...

The fatal flaw...

The industrial regime is motivated *only* by profit – nothing else matters. *Nothing else*. For two hundred years it has ruined, and it continues to ruin, millions of lives. It is at the brink of *destroying our biosphere*. Only an idiot or a lunatic can fail to see the human suffering and the destruction of our planet – our only home.

...

The diagnosis...

The logic is irrefutable. The industrial regime and its enforcer, the nation-state, are run by *sociopaths* – devoid of conscience, incapable of empathy, driven by greed, concerned *only* with their own personal material comfort.

BACKGROUND – They stop at nothing to maintain their lifestyle of excess. They have even rewritten history to keep us in the dark. Example – Robin Hood wasn't a romantic woodsman battling an evil Prince. He was the leader of an organized guerrilla movement. He was trying to stop the powerful and wealthy from clear-cutting Sherwood Forest. The authorities wanted to create pastures for the sheep that they needed for their profitable wool industries. History books are written by the winners, not the also-rans.

...

The distant past...

30,000 years ago things were different. We needed leaders who would ignore *everything* in their quest to further their interests, which often dovetailed with the interests of the tribe as a whole. The tribe's survival depended on its leaders' ruthlessness. The *worst* a powerful leader could do was destroy a valley, a hunting ground, a drinking well, a forest.

...

The immediate present...

Today they can destroy the planet. We can *no longer tolerate* sociopaths who are prepared to risk everything for their own personal material comfort. They are beginning to pose a risk to *the survival of our species*.

Evolution continues. The time has come. Their kind must be *culled* out of our gene pool. The interests of the sociopaths and the interests of the tribe have diverged.

We must put a human face on technology, machines, and industrial activity. We desperately need people who put humanity and its environment first – not subhumans who indulge *personal* greed at the expense of *mass* extinction.

...

The answer...

The sociopath must go the way of the dinosaur. His time has come and gone.

What is at stake is nothing less than the *survival of our biosphere* – and our species.

...

The way...

Each of us must play our small part. Small, but not insignificant.

Resist. Quietly. Individually. Effectively. Passively, or by direct action, whatever is your nature.

United in spirit we can make a difference. Divided we can do nothing. Look around you – one of the main ruses of the adversary and his goon squads is to *keep us apart* from each other.

We must alter the course of human history. We must re-establish a *timeline* that is healthy, positive, nurturing, sustainable.

Otherwise we lose the most important game of all – survival of the species.

Follow your heart and join the struggle.

In a nutshell, that is why *Spy & CounterSpy* is dedicated to fighting the goon squads of government tyranny and oppression.

Free F9 subscription...

F9 is a weekly email bulletin published by *Spy & CounterSpy*. It is distributed free to anyone interested in countersurveillance, antisurveillance, underground urban activist tactics, and tradecraft.

F9 promotes freedom and fairness in America. Subscribers include concerned citizens who simply want to enforce their right to be left alone. Subscribers also include activists who are working to change a system they see as unfair. Our list of readers includes advocacy groups, dissidents, patriots, journalists, civil rights groups, lawyers, disillusioned spooks, ex-cops, private investigators, ex-military, religious leaders, and many others.

***F9* is more than a newsletter.** The name *F9* is an acronym. It stands for federated freedom-fighter factions for forging fundamental fairness first. Nine words that start with the letter F. Hence, *F9*.

According to official topographical maps we're 9 miles across the Canadian border, 9 miles outside the reach of the FBI and NSA goon squads. So the numeral 9 is a very meaningful number for us.

When your application for the *F9* bulletin is received, you're automatically enrolled as a member of the *F9* organization. This is an informal and voluntary association of concerned American citizens. You become a *Double F* (a freedom-fighter for the organization). However, you're not under any obligation. Nor do you have any special privileges. Anything you do (or don't do) is up to you. That's because *F9* does not issue commands to its freedom-fighters. *F9* does not order, *F9* informs.

Each email address to which the bulletin is emailed is considered a *cell*. Whether you subscribe as an individual or as a group, you become a cell in *F9*. No cell knows any other cell's identity. If you apply for membership anonymously, even we don't know your identity (which is just fine with us).

Return to our home page and click on *Be a whistleblower* for more information on anonymous email.

What's inside the bulletin? Each issue of the *F9* bulletin contains one or more of these five types of articles – *Ask Agent X*, *SitRep*, *Underground Messenger*, *Communiqué*, and *Feature Editorial*.

Article 1 – *Ask Agent X*. You are invited to send questions about surveillance and tradecraft to *F9*. Answers to readers' questions are published in *Ask Agent X*. This column is a powerful tool for disseminating practical information to targets of surveillance. It helps build morale by showing that you're not alone in your struggle against the government's surveillance and repression goon squads.

Article 2 – *SitRep*. This series of articles is an up-to-the-minute situation report about our current countermeasures against FBI surveillance and dirty tricks. You'll read about specific campaigns being conducted against us by the FBI. The

actions of individual undercover agents will be analyzed and explained within hours of the actual event, including detailed physical descriptions of the agents involved. The *SitRep* series of articles is your ringside seat at our ongoing no-holds-barred match with the FBI – covering countersurveillance, antisurveillance, psy ops, and underground urban activist tactics. The *SitRep* series is practical, relevant, timely, germane. It's the most effective way we can help our many American friends. Because the FBI has no power of arrest and no right to carry handguns in Canada, their goons are *unable to intimidate us*. Consequently, we routinely make it a point to humiliate their agents by exposing and neutralizing their actions. As different intelligence agencies and security services enter the scene, you'll read about them too.

Article 3 – *Underground Messenger*. This section of the *F9* bulletin consists of messages to active *F9* cells. An active cell is one that has expressed interest in learning about *direct action*. Full instructions on how to become an active cell are contained in the *F9* bulletin. We have no way of knowing – *and we don't want to know* – whether you put into action what you read in *F9*. That's because *F9* doesn't order, *F9* informs. Becoming an active cell is not for wannabees or bystanders. It's for people who want to make a difference and help put America back on track. It's for people who – like the heroes and heroines of the American Revolution – are ready to answer the call of idealism and sacrifice.

Article 4 – *Communiqué*. This series of articles focuses on the bigger picture. It puts surveillance and oppression worldwide into perspective. It talks about theory, principle, politics, tactics, and strategy. The underlying theme of *Communiqué* might be stated as "when authority fails, repression begins". *Communiqué* discusses alternatives for society, government, and individuals – all within the context of freedom and fairness.

Article 5 – *Feature Editorials*. Every subscriber to the *F9* bulletin is invited to submit articles to be considered for publication.

Application for a free *F9* subscription

Personal information you provide is kept confidential. We are located just across the border in Canada (nine miles outside the reach of the FBI, BATF, DEA, and other goon squads). Items in red are required to process your application. Items in blue are optional and can be left blank if you wish. At a minimum, you must provide an email address and a nom de guerre.

[Web form omitted. If the authors have not revoked their PGP key (find it below), you can try to reach them by posting encrypted messages to them on Usenet. - P.]

...

...

...

About our workshops...

Spy & CounterSpy offers weekend workhops in tradecraft. Whether you simply want to defend your right to be left alone – or whether you're working to change a system you see as unfair – the workshops provide knowledge and skills you can apply right away. The workshops provide solutions to the problems faced by activists.

The problems. The authorities rely upon SSG and SWAT to maintain their rule of oppression. SSG stands for *surveillance specialist group* – that's spy-talk for a surveillance team. SWAT stands for *special weapons and tactics* – that's double-talk for a paramilitary death squad.

Together, these two forces have spelled ruin for underground activists in the USA. Simply stated, there has been no viable urban countermeasure against the *penetrating gaze* of SSG and the *massive firepower* of SWAT.

Until now.

The solutions. At the workshops you'll learn the new STING tradecraft. STING™ stands for *stealth-trained invisible new guerrilla*™. This system uses as a starting point the fundamental principles outlined by legendary urban guerrilla Carlos Marighella (1911-1969). Upgraded and adapted for today's hostile environment in America, STING is the only method that will consistently detect and neutralize SSG and SWAT. In other words, *stealth* is the only way to beat the surveillance teams and paramilitary assault forces that the authorities rely on.

Workshop location. The workshops are held at our offices in Victoria, British Columbia, Canada. We are located 9 miles across the border – out of reach of FBI, BATF, DEA, IRS, FEMA, and other goon squads. We're just a short ferry ride from Seattle, Washington.

Content. Our workshops are a mix of lecture, anecdote, exercise, and demonstration. You'll learn things that you cannot get anywhere else.

The table below shows a summary of the STING curriculum.

Topic	Contents	Details
Surveillance	1. Vehicle 2. Foot 3. Technical 4. Penetration	You'll learn about your adversary's capabilities, including vehicle surveillance (*wheel artists*), foot surveillance (*pavement artists*), technical surveillance (*bugs, video, phone taps, garbology*), and penetration techniques (*informants, agent-provocateurs, etc.*).
Countermeasures	1. SERE 2. Detection 3. Obstruction 4. Evasion	SERE is spy-talk for survival, evasion, resistance, escape. You'll learn to use *antisurveillance* to detect the goons. You'll learn to use *countersurveillance* to obstruct and harass them. You'll learn *evasion* techniques to give them the slip.
Resistance tradecraft	1. Set up a front 2. Go underground 3. Communication 4. Confrontation 5. Interrogation	You'll learn how to achieve your goals in spite of surveillance. Set up a front organization to cloak your activities. Manage your communications. Form cells that are resistant to penetration. Arrange secret meetings. Beat interrogation. Master one-time pads. Use elliptical conversation. Implement parcours de sécurité. Finance your operations.

...

Tuition. All our workshops are structured on a *pay-as-you-learn* basis. You take no risk. We teach you first *before* asking for your tuition. The fees we collect are used to finance our ongoing campaign against government tyranny in America.

You'll attend three workshops over Saturday and Sunday. Your tuition of $200.00 is payable at the end of each workshop. Your cost for the full weekend is $600.00.

US dollars. The printed manual is extra. Transportation, accommodation, meals are your responsibility.

Can't attend? Order the toolkit. This is the same printed manual that participants use at the workshops. It is an illustrated learning guide, a study resource, and a review aid. It is a manual for today's American urban guerrilla.

If you can't attend the workshops, reading the manual is not the same as being here, but it's *the next best thing*. Practical content with rugged cover and binding. Study it at your desk or carry it with you. Just $150.00 each. Delivered by regular mail or next-day courier. Vickie sends these out the week after the workshop. Attendees pick up their manuals when they arrive at the workshop.

Act now. Supplies are limited. Requests for the manual are filled on a *first-come first-served* basis. Act now to avoid disappointment.

US dollars. Regular mail delivery is included. Add $25 for next-day courier to any street address in the USA. Add $40 for courier to other countries. To order, use the registration form later in this document and choose *"Manual Only"*.

Victoria's inner harbor, visited by 35,000 American tourists each year.
In the foreground is one of the city's water taxis.

Cover. Victoria is a world-renowned tourist destination. It is visited by more than 35,000 Americans each year. This provides cover for your visit. Only we know you attended – you'll leave no paper trail for the goons to find – and we've got a short memory.

Schedule. The workshops are scheduled to fit inside your weekend. You don't need extra time off to attend. You can arrive Friday evening or Saturday morning, attend all three workshops, and depart Sunday afternoon or evening. Victoria is accessible by ferry, aircraft, and bus.

Our role. It is important to realize that we are not security consultants. We are victims of surveillance just like you – and we are investigative journalists. We limit our discussion to how we handle situations ourselves – we also reveal leaked information – and we talk about suppressed information we have uncovered. You'll see and hear presentations, demonstrations, case studies, role-playing, and Q&A sessions from someone who understands the physical and psychological pressure you face as a target of surveillance.

The table below shows your itinerary for the STING weekend.

What	When	Comments
Arrival	Fri. evening or Sat. morning	Your travel options include ferry, bus, and aircraft. Email Vickie for a list of transportation schedules and recommended hotels.
Workshop 1	Sat. afternoon 1 pm – 5 pm	Includes a mid-afternoon refreshment break. Prerequisite – You must have the workshop manual. Contents – Introductory Level surveillance and countermeasures.
Break	5 pm – 7 pm	Use this time to freshen up at your hotel or try one of Victoria's many restaurants.
Workshop 2	Sat. evening 7 pm – 11 pm	Includes a mid-session break with snacks and refreshments. Prerequisite – Attendance at Workshop #1. Contents – Intermediate Level surveillance and countermeasures, as well as Introductory Level resistance tradecraft.
Workshop 3	Sun. morning 8 am – 12 noon	Includes a mid-morning refreshment break. Prerequisite – Attendance at Workshop #2. Contents – Advanced Level surveillance, countermeasures, and resistance tradecraft.
Departure	Sun. afternoon or evening	Your travel options include ferry, bus, and aircraft. Email Vickie for a list of transportation schedules.

The workshop presenter. Your workshop leader is Lee Adams, the driving force behind the *Spy & CounterSpy* website.

Lee is a survivor of hostile surveillance and dirty tricks by numerous intelligence agencies and security services. Return to our home page and click on *About us* for additional background info.

The workshop facilitator. Your workshop facilitator is Vickie Nickel, survivor of four years of 24-hour surveillance by US Naval Intelligence, and a victim of a frame-up by Soviet Military Intelligence. Return to our home page and click on *About us* for more about Vickie's background.

Location. Victoria is wonderful in summer and fall. Warm, sunny, balmy. Even in winter it rarely freezes or snows here. The city offers everything from first-class accommodation to bare-lightbulb motels – the choice is yours. Whale-watching tours. Wilderness hiking. Upscale shopping. Horsedrawn carriage tours. Harbor water taxis. A vibrant night-life. To learn more, take a few moments and browse http://www.victoriabc.com.

NOTE – This is an external link, so you might want to bookmark this page before leaving.

Date. The next workshop weekend is scheduled for January **[SOLD OUT]**th. You can reserve your place by ordering your manual. Click here for our secure online registration form.

SUBMITTING THE FORM – You can either submit the form online, or you can print the form and send it to us by mail or fax. PRIVACY – If privacy is a concern, you should consider using a cybercafe and an anonymous email account. Return to our home page and click on *Be a whistleblower* for tips. ORDERING ONLY THE TOOLKIT – If you're not attending the workshops, you can use the online registration form to order only the manual. [Sorry, current printing is SOLD OUT.] NO SHOWS – If you register for the workshops and don't attend, we'll consider your order "Manual Only" and we'll mail your manual to you.

IMPORTANT – When you select our online form, you'll see a caution about the Site Certificate. Be sure this message says Web Communications (the server in California that hosts Spy & CounterSpy). This is your assurance that your information is being securely transmitted by encryption.

Questions? To find out more about the workshops – and to get a list of hotels and transportation options – click here to send email to workshop facilitator Vickie Nickel at training@bc.sympatico.ca. Telephone 250-475-1450. Fax 250-475-1460.

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."

Lee Adams KeyID 0x9C23BED4 - 3072/1024 DH/DSS

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP for Personal Privacy 5.0

mQGiBDUcbvERBADkP607T6qK5JqlRlo1uAs/xNQvc90BYoiqd3AE2kHXX4cAa16T
oi0Yt/kT8jstFXzbJx0Z1M+bTxmFZGZOjodPdLJE5PeEH5Y8iKcBfYYW8zyZW6i7
LNf6NEtXGdzL7eFXiw37Cb0mOqdJ3AMvyt9B6pQUCNhu24MaDz/p01WL1wCg//jj
QQYXvEZSwUEsGqLdyguRx3cD/08OztFD6skbBVA+ewSildAINMD0QKFATrFsXKcq
FztLZyDy9tRJ2mSqaBucHqEiefNBV+RQb7rUp/IeUDL+uMeB9SK1n82e2VNx5SA9
Hw/1fVQDDRCG9lrEBLlGqtWjQCdN8jQA4+R8yUYfKrYOYtKbAixiFSMcroleEIzh
Qxk2BACxf96TYXC7h7XioDrXLGyVuKhC4z9XzlguLLqQ3G1tfVRyY3VSwXW1gQMg
IyxcB5C/OHNw5Cm1dr1aArqo6/DuveM9ffT/cZOasy5gPLaTU5fRNTgV/aXqPl9+
leT7AxvPrE7SuPPesNotX3Qy0Hpi//zk6afZQPsr8tHzmifeVrQkTGVlIEFkYW1z
IDxlZGl0b3JAc3B5Y291bnRlcnNweS5jb20+iQBLBBARAgALBQI1HG7xBAsDAQIA
CgkQFXqepZwjvtSq9wCgh+b9s7Cx1fZji0RKC8xRwNL6tIoAn1WhUuNUwD6/cEqc
kr1EKHN3TtVduQMNBDUcbvIQDADMHXdXJDhK4sTw6I4TZ5dOkhNh9tvrJQ4X/faY
98h8ebByHTh1+/bBc8SDESYrQ2DD4+jWCv2hKCYLrqmus2UPogBTAaB81qujEh76
DyrOH3SET8rzF/OkQOnX0ne2Qi0CNsEmy2henXyYCQqNfi3t5F159dSST5sYjvwq
p0t8MvZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU6Y9AVfPQB8bL
Q6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN/biudE/F/Ha8
g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9WE5J280gtJ3k
kQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0/XwXV0OjHRhs
3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQmwJG0wg9ZqRd
QZ+cfL2JSyIZJrqrol7DVelMMm8AAgIL/1jmtN8xWpX7cZ7CSjTVr3/mjkqzARDy
ma175KpXSN9tGHa+XgAatDk4lc0SsXPKpAlRfx2C8Ek94HrS0YjoarOx8JqfMsL7
N+jQgtdKlOCyy+PtgBmAMJ3YYuuN5JrY+RNMn7TJ/XVVjRK7AqoP2gz/lay802xQ
mXV0UTiqCsd4ErSfOA5oR0exfQbRMCbwwWL5mUeopDsKY906n+NK2mavugdW89Tz
wVDPXUECUKZ3dnEFrhiR34V9pIghctr37BtL43jekFj8J8NaGzLQ6FUhIVgkDt2D
XH7xC6S3NMskieUtx14bLi3lmN2RdzsjTt2ac+5JlaHCHW/pWux7CQRngbfulQn6
QLfJUPYrP47NUzhn7D0525dqL/pTgTUVrJIsAPA8W8wAlDpl43HbBO+Z1u/IMXzj
ySHdWfYAW77dxY6VFyl6e0RD00whNlsTCKLJLROrYuFlAQeEnUGMm7GXknHXlzkb
j+AIV9uig7Hjnnf6SQQvvmig0im8V3v+s4kAPwMFGDUcbvIVep6lnCO+1BECm24A
oJ/N8/fmN/6acP8SGodNvPs3q9kUAJ4xME10DJjAUGz7284QMNPSDq6Nog==
=lgfJ
-----END PGP PUBLIC KEY BLOCK-----

...

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.

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 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.

Providing knowledge and skills to supporters of freedom and fairness.

A source of knowledge and skills for the new American patriot.
Frank talk about resistance strategies, urban guerrilla tradecraft,
countersurveillance techniques, and underground activist methods.

F9 Bulletin is a free publication from the publishers of Spy & CounterSpy
-- "spy school for the rest of us". Contents Copyright 1998 Lee Adams.
All rights reserved. Quoting and copying prohibited. Published weekly
by Here's-how, Right-now! Seminars Inc., PO Box 8026, Victoria BC, Canada
V8W 3R7. Telephone 250-475-1450. Fax 250-475-1460.
URL http://www.spycounterspy.com

F9 stands for Federated Freedom Fighter Factions For Forging Fundamental
Fairness First. F9 is an informal and voluntary association of American
citizens concerned about the escalation of government tyranny.

In accordance with Title 17 U.S.C. section 107, this material is distributed without profit or payment to those who have expressed a prior interest in receiving this information for non-profit research and educational purposes only.

Disclaimer: F9 does not issue orders or make suggestions; F9 merely informs. We do not endorse, condone, or encourage illegal activity. The material in F9 is presented for information, research, entertainment, and education purposes only. Pronouns such as you, your, our, and we are used for ease of readability only. Terms such as guerrilla, partisan, commando, raiding, quick reaction force, and active cell refer to states of mind during lawful dissent, not operations or actions.

* * * F 9 B U L L E T I N
Volume 1 Number 1 September 17th, 1998

* * * I N S I D E T H I S I S S U E

* * * P L A Y I N G B Y T H E R U L E S

This is the first issue of F9 Bulletin. This publication is an adjunct to our Spy & CounterSpy website. The website promotes freedom and fairness.

In particular, it teaches people to resist what many citizens see as government tyranny and oppression. The website provides free tutorials in countersurveillance, antisurveillance, and underground urban activism.

Because the Spy & CounterSpy website is on the worldwide web, it is available to anyone and everyone. However, not everyone is ready for its message. The articles at the website are by necessity toned down and sanitized.

The email message you're reading now, F9 Bulletin, on the other hand, is specifically intended for readers like you who want a frank, tell-it-like-it-is approach. And that's exactly what you'll be getting in this publication.

Countersurveillance and antisurveillance are profound topics, but there is a bigger picture. If you haven't done so already, please take a moment and familiarize yourself with the political position of Spy & CounterSpy. Simply go to our home page at http://www.spycounterspy.com, scroll down to the final paragraph before our sign-off logo, and click on "political position". Alternatively, you can point your browser directly at http://www.spycounterspy.com/manifest.html.

If you CANNOT reconcile our political position with your own, then perhaps F9 is not for you. Which raises the question, which of our two tenets are you against -- freedom or fairness? (Of course, this is the same question we ask the various public libraries in the USA that block our site.)

On the other hand, if you DO agree with our political position -- or at least accept our right to hold such a position -- then we heartily welcome you as a fellow freedom-fighter. An enemy of government tyranny is a friend indeed.

In return for the practical tutorials and confidential information you'll be receiving in F9 Bulletin, we ask only one thing in return. Please DO SOMETHING with the knowledge and skills you'll be learning.

You CAN make a difference. But only if you act. Simply reading isn't good enough. With knowledge comes responsibility. There are three ways you can become part of the solution. Choose the way that best suits your temperament -- we've listed them here as good, better, and best.

GOOD -- Tell others about the web site. Help open their eyes. Get them thinking. Make them aware of what's really happening.

BETTER -- Form a cell. Get people involved in planning, organizing, and supporting each other. Put into practise some of the skills you've learned from the Spy & CounterSpy website. The way things are going, you may soon need those skills.

BEST -- Direct Action. You are a member of F9. Remember, F9 doesn't issue orders, F9 merely informs. It's up to you to read between the lines. Decide what needs to be done. Then do it. Help put America back on track. Like the heroes and heroines of the American Revolution, it's time for you to answer the call of idealism and sacrifice. If you love your country but fear your government, then perhaps Direct Action is for you.

* * * T I M E W A R P 1 9 3 8 - 1 9 9 8

Many people don't realize that during the 1920s and 1930s the world was involved in a profound struggle between two ideologies -- fascism and communism. Stalin's implementation of communism was nasty. Hitler's implementation of fascism was ugly.

America went to war and defeated Hitler's fascism. That left the specter of Stalin's communism. After thirty years of Cold War, the USA finally vanquished Soviet Russia's style of communism.

But all this came at a price.

Yes, we defeated fascism in 1945. But our bureaucrats were seduced. Their minds had been infected. They became entranced by fascism's promise of power over the people. Drawing on lessons learned from the Nazis, our bureaucrats began to develop systems for controlling the population.

Fast-forward to 1967. I remember a teenager who used to shovel snow during the winter at a senior citizens' complex in a place a lot like the cities in North Dakota. The building manager was a kindly old gentleman named Bill. He was a good role model for the young fellow who shoveled snow. Bill was an immigrant from the old country. He was from Germany. He was honest. He was decent. He had ethics.

He also had a history.

Flash-back to 1936. Bill had become concerned at what Hitler was doing to his country. So Bill became an activist. In the spring of 1938 the goons came an hour before dawn and kicked in the door. Bill was arrested by the Gestapo. But Bill's sister was dating a lawyer. The lawyer got Bill off on a technicality. Bill realized he'd never get a second chance, so he went underground. He stayed there for all of World War II, leading a resistance movement, living on his nerves. In 1945 the US Army showed its gratitude by offering to make Bill interim major of the newly-liberated city of Cologne, Germany. Bill declined. He'd had enough. He emigrated to Canada instead, where a teenage boy I once knew ended up shoveling snow for him after school.

Bill is gone now, and I miss him. I often ask myself what Bill would think of the political situation today. I expect he might notice the parallels between fascist Germany 1938 and fascist America 1998. I like to think that Bill would recommend getting involved, making a difference, perhaps going underground. He might suggest that we pause and reflect on what's happening in the USA today -- national ID cards, police terrorism, oppressive taxation, unresponsive elected officials, rampant surveillance, no-knock warrants, a tethered news media, a disgraced (but still arrogant) national leadership, the list goes on and on.

* * * C L O S I N G N O T E

Is F9 for you? Should you get involved? Only you can answer that question. Look deep in your heart and decide if you've had enough of the brutality and unfairness of a system that many decent Americans are beginning to find morally repugnant and intellectually embarassing.

Is F9 for you? Should you get involved? We are all outlaws already anyways. Look around you at the thousands of laws, statutes, regulations, and rules. Any bureaucrat who wants to can get you. Any cop worth the badge can find something to arrest you for.

Is F9 for you? Should you get involved? Remember that you are not alone. More and more, concerned citizens across America are beginning to adopt a personal philosophy of "no fear, no mercy, no limit".

NO FEAR -- of the heavyhanded tactics of authorities acting unlawfully.

NO MERCY -- for the oppressor, or for those who have sold us out.

NO LIMIT -- to our courage and resolve. Winners never quit, and quitters never win. In the end we shall prevail.

* * * W H A T N E X T ?

To continue to receive F9 Bulletin by email, you must reply with "Continue F9" in the subject line and your nom de guerre and email address in the body. The best way to do this is to click the Reply button of your email program while you're online. Or else send email to F9's subscription manager Vickie Nickel at training@bc.sympatico.ca

Do it now. If you don't reply you will not receive the next issue of F9. You must reply after each issue of F9 Bulletin.

The next issue will be out a week from now. You can expect articles, tutorials, and exposes that pull no punches about countersurveillance, antisurveillance, and underground urban activism. If you want the plain, unvarnished truth about how all this stuff really operates, you won't be disappointed.

Cheers.

From your friends at http://www.spycounterspy.com

* * * F 9 B U L L E T I N
Volume 1 Number 2 September 24th, 1998

* * * I N S I D E T H I S I S S U E

* * * F B I A R R E S T P R O C E D U R E

You're probably already aware that the Spy & CounterSpy website is currently featuring a series of articles about FBI vehicle surveillance techniques. What you probably don't know is that we're holding back a lot of information because we consider it too sensitive for public consumption. However, as a subscriber to F9, you'll have the opportunity to get the whole story.

Quite often the FBI must arrest a suspect who is in a vehicle. When it comes to FBI arrest procedures, don't believe what you see on TV.

In real life, it is not typical for FBI Special Agents to force a suspect's car off the road, then leap from their car with handguns drawn, shouting, "Keep your hands where I can see them! Now get out of the car!"

This scenario often ends in a shoot-out, where the FBI runs the risk of losing evidence, suspects, and agents.

What you're about to read next was told to us by someone who was on the receiving end of a vehicle arrest situation.

Our informant, whom we'll call Citizen A, was the driver. An acquaintance, whom we'll call Citizen B, was in the passenger seat.

Seeming to come from out of nowhere, two FBI bucars pinned Citizen A's car. (Bucar is slang for a bureau car -- an FBI vehicle.) One FBI car stopped broadside immediately in front of Citizen A's car. A second FBI car pulled up immediately behind Citizen A's car.

Even before the first FBI bucar had come to a full stop, Citizen B in the passenger seat realized they were about to be arrested and began shouting, "Go! Go! Go!"

But it was already too late.

An FBI agent leaped from the bucar in front. He was carrying a standard police flashlight. (These are available on the open market under the MagLite(tm) brand name). They are big, heavy tools -- built more like a club than a flashlight.

The FBI agent stepped up to Suspect A's car and with two swings smashed in the windshield. A moment later he had one hand around Citizen A's throat. With his other hand he held a handgun to Citizen A's head. He was shouting "Keep your hands on the steering wheel."

Our informant told us that he'll never forget the feeling of broken glass in his hair and down the back of his shirt.

Of course, while all this was happening to Citizen A in the driver's seat, exactly the same thing was happening to Citizen B on the other side of the car. Another FBI goon, another flashlight, another quick entry through the windshield.

The entire arrest took less than 5 seconds.

As you probably already know, windshields are made of laminated glass. It breaks into rounded pebbles that won't cut the occupants of the car. A couple of vigorous whacks from a police flashlight and the entire windshield falls away. The visual shock and the noise will terrorize and freeze the occupants, giving the FBI thugs time to get their hands inside the car and apply "physical restraint" (that's polite talk for grab-you-by-the-throat).

The lesson? Don't think of your vehicle as a sanctuary. It's more like a holding pen when the FBI's goon squads are nearby.

Clearly, this is not a game for choir boys.

* * * S I T R E P

(SitRep is shorthand for situation report.)

ITEM #1 -- AUSTRALIA.
It has been reported to us that the Australian Security Intelligence Organization (ASIO) is compiling dossiers on many Australian citizens in preparation for the upcoming Olympics. It seems that if you so much as jaywalk the ASIO goons consider you a potential terrorist.

ITEM #2 -- SWEDEN.
We've received reports that Sweden's security service, SAPO, is in the process of hijacking Swedish airports. SAPO is taking over administration functions, sacking long-term employees whom they consider a security risk, and replacing them with SAPO operatives. It seems that belonging to any political party other than the two mainstream parties is enough to get a person dismissed. Public outcry is rising, but the government is stonewalling and refuses to open an investigation into abuse of authority by the SAPO goons.

ITEM #3 -- EMAIL ENCRYPTION.

Here at Spy & CounterSpy we're testing a new email encryption system called InvisiMail. It is based on the RPK mixture generator, whose exponentiation math is as strong as PGP's. The software uses a hands-free approach. The program runs in the background and automatically takes care of exchanging public keys with recipients. If they've got InvisiMail, the software encrypts your message automatically. If they don't have InvisiMail, the software sends your message as plaintext. As an F9 subscriber, you may want to check out this new system. A free version can be downloaded from http://www.invisimail.com. You can also download from http://www.rpkusa.com. RPK encryption was developed in New Zealand, away from the prying eyes of the FBI, NSA, CIA, and others. It is not subject to any heavyhanded export restrictions. The patent-protected algorithm is available for inspection -- they're offering a $10,000.00 reward to anyone who cracks RPK's binary keystream generator.

* * * N E W A R T I C L E S

Don't forget to keep visiting the Spy & CounterSpy website regularly at http://www.spycounterspy.com.

A number of new articles have been recently posted, including...
Spy address book
Tax resistance primer
Arrange secret meetings
FBI vehicle surveillance 2
Use dead-letter boxes
Be a whistleblower

You'll also want to check the Glossary at the website regularly. It's always under construction, with new terms and definitions being added every few weeks.

* * * P A R T I N G S H O T

To continue to receive F9 Bulletin by email, you must reply with "Continue F9" in the subject line. Please include your nom de guerre and email address in the body. The best way to do this is to click the Reply button of your email program while you're online. Or else send email to F9's membership manager Vickie Nickel at training@bc.sympatico.ca We have adopted this proactive policy in order to reduce the chance of F9 being sent to someone who doesn't want it. This policy also makes it easier for you to change your email address if your cell has been compromised.

The next issue will be out a week from now. You can expect more frank talk about countersurveillance, antisurveillance, underground urban activism, and tradecraft. If you want the plain, unvarnished truth about how all this stuff really operates, you're reading the right newsletter.

Cheers.

From your friends at http://www.spycounterspy.com

Lee, Vickie, Agent X, and our network of whistleblowers

* * * F 9 B U L L E T I N * * *
Spy school for the rest of us.

Volume 1 Number 3 Thursday, October 1st, 1998
A free publication from <http://www.spycounterspy.com>

* * * I N S I D E T H I S I S S U E

* * * F O R F E I T B Y D E F A U L T

Nobody ever scored a winning goal from the spectactors' seats.

Stop for a moment and think. The spectators don't determine the final score, the players do. How can you change the outcome if you're not even in the game? You gotta get out on the playing field if you want to make a difference.

Let's not mince words. The oppressor's deliberate campaign of terror has worked. The government's excessive application of force has cowed many people who would otherwise get involved in resistance against government tyranny.

Simply put, the strategy of the goon squads is to keep you off the playing field. They do this by intimidation. They do this by terror. They do this by arbitrary arrest. They do this by arbitrary sentencing.

It's a time-warp. 1938 and 1998. Stop and think. The SS and the Gestapo used exactly the same tactics.

But Americans are made of sturdier stuff.

At some point a courageous minority will begin to stir, just like the heroes and heroines of the American Revolution. They will look deep in their hearts and they will decide it is time to answer the call of idealism and sacrifice.

This small, but growing, constituency will decide they've had enough of the brutality and unfairness of a system run by thugs who have suborned the US Constitution for their own purposes, creating a system that many decent Americans find morally repugnant and intellectually embarassing.

The courageous minority will continue to visit websites like Spy & CounterSpy to get the resistance skills they need. They'll subscribe to publications like F9 in order to find articles that inspire, motivate, teach, and compel them to act.

Should you get directly involved? Only you can answer that question.

Remember, each of us can make a difference. But only if we act.

It's time for us to start affecting the outcome of the game. The goon squads have had the playing field to themselves for too long. It's time for us to vacate the spectators' stands and take our rightful place on the field.

The consequences of this line of reasoning are profound. Simply reading F9 isn't enough. With knowledge comes responsibility.

There are three ways each of us can become a player. Each of us must choose the way that best suits us.

ROLE #1 -- BECOME A SYMPATHIZER. Tell others about the Spy & CounterSpy website at http://www.spycounterspy.com. Open up their eyes and get them thinking. Start planning ahead. Get a sense of direction and purpose. Continue to live your normal life, but adopt a nom de guerre and start creating an identity that cannot be traced or located by the authorities. Start caching items you may need later. Learn communication skills -- arranging secret meetings, using dead-letter boxes, sending anonymous email, etc. Consider forming a cell and recruiting members. (See our website at http://www.spycounterspy.com for tutorials about these skills and others.)

ROLE #2 -- BECOME A SUPPORTER. Form a cell and become involved. (We'll be posting a new article at the website showing exactly how to set up the links between members, cells, and circles in an underground resistance movement.) Your cell can begin propaganda -- informing others about the misinformation campaigns of the authorities. You can also begin defensive operations -- warning or assisting persecuted persons and publicizing the excesses of the government's goon squads. Your cell can also begin teaching the general population how to behave towards the authorities -- passive civil disobedience, quiet protest, non-fraternization, non-cooperation, ostracizing of government employees, and more.

ROLE #3 -- BECOME AN ACTIVIST. Decide what needs to be done. Then do it. Show your patriotism and loyalty by becoming an urban guerrilla. Help put America back on track. Use Direct Action. Your cell can go on the offensive with operations like letters to the authorities, tax resistance, embargo, boycott, agitation, protest, petitions, voter recalls, civil disobedience, and monkey-wrenching. (Monkey-wrenching means it's impossible to tell if it was intentional or accidental, deliberate, or forgetfulness, incompetence or oversight.) Your cell can undertake counterintelligence operations to isolate informers, agent provocateurs, moles, and collaborators. You can also undertake actions that will invite coverage by the news media. (But remember that F9 does not encourage or condone unlawful operations like sabotage, kidnapping, assassination, terror, etc.)

Is Direct Action for you? To find out, look in your heart and ask yourself the following question. Do I love my country but fear my government? Answer one question and you've answered the other.

In coming issues of F9 Bulletin, you'll see how to start receiving coded messages for your cell from F9. You'll see how to plan your work and then work your plan.

* * * T H E C O N T A G I O N E F F E C T

During resistance against government tyranny, the impact of your actions is leveraged by the news media. This means you are affecting the situation in a number of different ways. This is called the Contagion Effect by researchers. In other words, the actions of your underground group are contagious. Here's why.

First, your action boosts the spirits of other citizens who are considering getting involved. It builds morale among like-minded citizens.

Second, your action provides inspiration for others. It motivates "copy-cat" acts of resistance. It shows others what can be done. It shows other citizens that they are not alone in their thinking.

Third, your action provides a diversion. This benefits other cells. While the attention of the authorities is focused on your action, other resistance groups will find it easier to research, plan, rehearse, and carry out their mission without being detected.

All of this leverage, however, is dependent upon news media coverage of your action. This formula has not been lost on the bureaucrats. A recent study was conducted of resistance movements and their relationship with news media. The study investigated the four major American TV news networks and nine major international daily newspapers. Here's part of what the bureaucrats learned:

LESSON #1 -- The major TV networks (ABC, CBS, NBC, and CNN) covered about 18% of all politically-motivated acts by resistance groups. This means one in five actions makes it onto the supper news.

LESSON #2 -- The nine major international daily newspapers covered about 30% of all politically-motivated acts by resistance groups. This means one in three actions received "ink", as newspaper reporters are fond
of saying.

LESSON #3 -- Perhaps most important, the study found that actions receiving coverage in the news media were followed by "copy-cat" actions. This happens more often when the action receives coverage.

The lesson is obvious if you're considering Direct Action. In addition to the direct impact of your act, there is a powerful ripple effect.

The authorities don't want you to know any of this, of course.

Nor do they want you know about the so-called Blackmail Effect. Numerous resistance movements worldwide have used this subtle strategy to considerable effect in getting their message across in spite of an antagonistic, tightly-controlled media.

Here's how the Blackmail Effect works. If a news media outlet refuses to cover the actions of a resistance group, the group lets it be known that actions will be escalated until news coverage begins. The responsibility for damage and injury is laid at the doorstep of the recalcitrant journalist or editor. A compromise soon occurs. The resistance group gets the "coverage" it needs. The news media gets the "sensationalism" it needs.

Again, the authorities don't want you to know any of this, of course. But you'll continue to learn about these and other items in F9 Bulletin.

* * * B L O W B A C K
(Letters from readers. Blowback is spy-talk for unexpected backlash from covert ops. Readers' comments are edited for brevity and style.)

BLOWBACK ITEM #1 -- WINDSHIELDS
A number of readers responded to our September 24th article about the FBI's vehicle arrest technique. As you probably remember, the article described how FBI agents use heavyweight flashlights to break in through the windshield before the suspect has time to react.

An ex-cop writes -- "During the years I was in law enforcement we were allowed to use slapjacks and blackjacks (lead-loaded saps), but due to the tremendous amount of physical damage and death they were prohibited in the 1970s. This is when the Mag-Lite made its appearance. Crafted of heavyweight aircraft

aluminum, it could do the same damage but with the innocent appearance of a flashlight. Your article is quite correct."

Another reader writes -- "A technical correction. Side and back windows are made of tempered glass that crumbles into oblique (safe) pebbles. Windshields are made of laminated glass that is designed to resist penetration. Windshields will not yield to repeated blows from a hammer, much less a whack from a maglite. The entry is through a side window, not via the windshield."

BLOWBACK ITEM #2 -- FASCISM

A number of readers responded to our September 17th article titled "Time Warp 1938-1998". As you probably remember, the article described the struggle between democracy and fascism and communism in the 1920s and 1930s. It went on to describe the idealism of a resistance leader we knew -- he fought underground for the duration of World War II.

A reader writes -- "Fascism was an Italian political philosophy that advocated the concept of the corporate state. The philosophy of Adolf Hitler and Third Reich Germany was National Socialism, which advocated the primacy of race. These are two very different political views. It is my contention that historical accuracy should be of the utmost consideration, especially in a publication as controversial as the F9 Bulletin."

F9 responds -- With the advantage of hindsight, a growing number of historians are beginning to categorize Hitler's regime as being essentially fascist with a veneer of racial supremacy. In other words, same wine, new bottle. We're glad our reader took the time to write us. The reader is right, of course. But the historians who call it fascism are right too.

* * * J O I N T H E S E A R C H

Here at Spy & CounterSpy we're trying to get our hands on a copy of "Mini Manual of the Urban Guerrilla", by Brazilian freedom-fighter Carlos Marighella (occasionally spelled Marighela). The manual, containing 41 chapters, was originally published in Tricontinental Monthly in January 1970. It is now a collector's item.

If you know of anyone who has a copy, would you please have them get in touch with F9 membership manager Vickie Nickel at training@bc.sympatico.ca

This manual has been banned in many countries, for obvious reasons. Oppressive governments masquerading as democracies don't like it. Abusive bureaucrats masquerading as public servants don't like it. Goon squads masquerading as law enforcement don't like it. You get the picture.

Any tips or leads would be appreciated. An anonymous package would make our day. Our courier address is 3273 Tennyson Avenue, Victoria BC, Canada V8Z 3P4. Our mailing address is PO Box 8026, Victoria BC, Canada V8W 3R7.

Please spread the word.

[Marighella's *Mini Manual of the Urban Guerrilla* is reproduced in full as an appendix to this e-book. – Phosphor]

* * * P A R T I N G S H O T

To continue to receive F9 Bulletin by email, simply do nothing.

To cancel your subscription, reply to this email with "Remove" in the subject line. Please include your nom de guerre and email address in the body.

(TIP: You should promptly cancel your subscription if you detect new surveillance. This will help you deceive the goons into thinking that you are just one of the sheep. Watch mindless TV programs and read mindless magazine articles for a while too. The goons will soon lose interest and downgrade the surveillance. Vickie will gladly email you all the back issues when you renew your subscription.)

Questions, comments, and suggestions about F9 Bulletin can be sent to F9's membership manager Vickie Nickel at training@bc.sympatico.ca

The next issue will be out a week from now. You can expect more frank talk about countersurveillance, antisurveillance, underground urban activism, and tradecraft. If you want the plain, unvarnished truth about how all this stuff really operates, you're reading the right newsletter.

* * * F 9 B U L L E T I N * * *
Spy school for the rest of us.

Volume 1 Number 4 Thursday, October 8th, 1998
A free publication from http://www.spycounterspy.com

* * * I N S I D E T H I S I S S U E

* * * H O W T O B E A T S W A T

To enforce his reign of tyranny, the oppressor relies on SSG and SWAT. SSG stands for Surveillance Specialist Group -- that's spytalk for a surveillance team. SWAT stand for Special Weapons and Tactics -- that's doubletalk for a paramilitary death-squad.

Over the years, SSG and SWAT have gone by many different names. But a goon by any name is still a goon.

Up to now, the lethal combination of SSG and SWAT has proven disastrous for underground activists and their movements in the USA.

Is SWAT effective? Yes.

Does it get results? Absolutely.

Is SWAT invincible? No.

Despite their massive firepower and use of brute force, SWAT teams have weakness that can be exploited.

A typical SWAT element is composed of five people -- a Team Leader, a Scout, a Backup, and two Assaulters.

The Team Leader is the most experienced of the five. He is the nerve center and tactical command of the team. The Team Leader is in direct voice-contact with the other four members of the SWAT element, who each wear a hands-free UHF transponder with an earpiece and a throat-vibration microphone.

The Scout performs on-scene reconnaissance. The Backup carries a 12-guage riot shotgun. He provides security for the Scout. The two Assaulters each carry Heckler & Koch 9mm MP-5 submachine guns. All members of the SWAT element usually carry handguns, often a .45 or 9mm semi-automatic pistol.

SWAT members often wear balaclavas for the purpose of intimidating suspects and bystanders. The balaclava also keeps them anonymous -- this is handy because they reside in the same communities whose citizens they execute.

SWAT members wear military helmets and bullet-resistant body-armor. These guys are goons in the true sense of the word. They'll kill you and go for lunch five minutes later. It's nothing to them. Because of their myopic training, they figure the solution to every problem is massive application of force, preferably lethal.

Once it's arrived on the scene, SWAT never withdraws.

In a typical call-out, the SWAT element is reinforced by duty police officers who form a containment perimeter at a distance from the suspect's location. Police snipers may also be present. More than one SWAT element may be on the scene. A Crisis Negotiation Team (CNT) is often mustered. CNT is somewhat of a misnomer, because their actual role is to obtain intelligence for an assault by SWAT -- and to fatally distract the suspect in the moments preceding the assault. Ambulance and Fire personnel are also usually deployed.

SWAT WEAKNESS #1 -- LACK OF MOBILITY. Their combat gear prevents them from sprinting long distances in pursuit of a suspect fleeing on foot. A number of suspects have escaped in exactly this scenario. This is the reason behind the containment perimeter. The regular cops pin you inside the "holding pen" while the SWAT goons methodically stalk you and then dispatch you, preferably from behind.

TACTICAL RESPONSE #1 -- If you know the terrain, you'll often be able to beat the containment ring. The cops on the perimeter cover the escape routes and checkpoints. The ring has gaps you can exploit. The cops seldom cover hidden routes that the only the local residents know about. Do your homework. Gather accurate intelligence. And rehearse, rehearse, rehearse.

SWAT WEAKNESS #2 -- THEY DON'T THINK. Their training has ingrained them with the mindset that the solution to every situation is force. SWAT is not motivated or inclined to negotiate or compromise. And
they never withdraw.

TACTICAL RESPONSE #2 -- Plan your operation so that political considerations and/or public relations are more attractive to the authorities than a lethal resolution of the crisis by SWAT.

SWAT WEAKNESS #3 -- OVERHEATING. Their balaclavas, gloves, shooting goggles, helmets, and combat fatigues mean that they can easily overheat in urban situations. It doesn't take much activity to get them sweating. Literally.

TACTICAL RESPONSE #3 -- Plan an operation that will require lots of physical movement by the SWAT members. Give them lots to crawl over, through, and around. Even big tough guys don't have much stamina when they start to overheat.

SWAT WEAKNESS #4 -- PERIMETER OVER-RELIANCE. They always set up perimeter control. They have become dependent on the "holding pen" strategy.

TACTICAL RESPONSE #4 -- Post an accomplice (ie sniper) outside their perimeter and SWAT becomes vulnerable to a flanking attack.

SWAT WEAKNESS #5 -- ONE TRICK PONY. They are trained to attack fixed targets. They are befuddled and confounded by a moving target. Especially a target they are continually losing contact with.

TACTICAL RESPONSE #5 -- Hit and run. Hit and run. Hit and run. Then disappear. Your key to tactical success consists of carefully planned escape routes, accomplice drivers, and prearranged support (ie hiding) from the local population.

SWAT WEAKNESS #6 -- LACK OF INDIVIDUAL INITIATIVE. Without their body-rig communication sets, SWAT members are lost. UHF frequency range is often less than a mile. Range deteriorates in locations with reinforced concrete and metal debris.

TACTICAL RESPONSE #6 -- Forcing or duping a SWAT member to transmit bogus messages over his transponder is an effective tactic for disorienting the entire team. Seizing a transponder and issuing your own messages is effective psychological warfare. Your voice is right inside their heads -- and these guys aren't exactly the brightest specimens our species has produced. Selecting a location that interferes with UHF transmission is a sound tactic.

---

3 RULES FOR BEATING SWAT:

RULE #1 -- Surround the SWAT element, including its perimeter force.

RULE #2 -- Fight scattered, never in a compact body.

RULE #3 -- When attacked, never stand and fight. Retreat, then counterattack.

Some resistance movements hold the view that if surrounded, you should immediately pick the weakest point, focus on it, and make a determined effort to break out. The resulting break in the enemy's line will produce two exposed flanks which you can counterattack, possibly more.

Savvy readers and students of American history will recognize these tactics as the same as those used by the natives to maul the British Regular Army in the 1600s and 1700s in colonial America.

All things considered, however, your greatest single asset is your ability to choose the location. This means planning ahead. It means being a moving target. It means not sleeping where SWAT can find you.

Heed the warning in the training manual of the Provisional IRA -- "Get your defense before you get your offense."

And remember that F9 does not endorse, condone, or encourage illegal activity.

* * * C A L L F O R C E L L N E T W O R K S

The American Revolution offers many lessons for today's activist. The heroes and heroines of the Revolution can provide inspiration and guidance to us all. They believed first and foremost that it is the right of every person to revolt against tyranny and oppression.

When you form your cell, you might want to consider affiliating it with one of the following networks that are being formed up. Each network of cells is named after a hero of the American Revolution.

A cell will specialize in -- but isn't limited to -- the functions made famous by the hero whom the network is named for.

Each cell chooses, plans, and carries out its own operations, of course. The network to which your cell belongs is a reflection of your personal temperament, strengths, and objectives in the struggle against government tyrrany. It is important to remember that F9 does not endorse, condone, or encourage illegal activity.

Some of the network affiliations are suited for one-person cells. Some are suited for cells with three or more members. Some are suited for ex-military types and ex-cops. Some are suited for self-taught underground activists and urban guerrillas. Some are suited for survivalists. Some are suited for loners, some are for joiners. Some cells are for people of action. Other affiliations are more suited for thinkers and planners. Whatever your background, whatever your goals, there's a network for you.

THE GEORGE WASHINGTON NETWORK OF CELLS -- Cells in this network specialize in classic guerrilla operations, like those of master tactician George Washington and his "Continental Army".

THE FRANCIS MARION NETWORK OF CELLS -- Cells in this network specialize in unorthodox partisan-type operations, like those of "The Swamp Fox", wiry little Francis Marion.

THE ETHAN ALLEN NETWORK OF CELLS -- Cells in this network specialize in daring, lightning-quick commando operations, like those of cunning Ethan Allen and his hardy "Green Mountain Boys".

THE JOHN PAUL JONES NETWORK OF CELLS -- Cells in this network specialize in raiding operations, grabbing or sabotaging the materiel and resources of the enemy, just like opportunistic John Paul Jones and his marauding raiders.

SAMUEL FRANCES CELLS -- Cells in this network specialize in double-agent operations, agent-in-place operations, and intelligence penetrations. This is ideally suited to cells composed of a single individual. Samuel Frances, known as "Black Sam", used his tavern to provide lodging and meals to the enemy forces while at the same time secretly sending valuable intelligence about their plans to George Washington during the American Revolution.

THE PAUL REVERE NETWORK OF CELLS -- Cells in this network specialize in early-warning alerts, like Paul Revere and his network of patriots.

THE THOMAS PAINE NETWORK OF CELLS -- Cells in this network specialize in propaganda. This can include posters, pamphlets, publishing, letters, wall slogans, radio call-in programs, impromptu forums, neighborhood meetings, and more. Like the stirring broadsheet articles of Thomas Paine, these cells strive to inform and stir the general public.

SONS OF LIBERTY CELLS -- Cells in this network specialize in street tactics. Like the "Sons of Liberty" street mobs in the weeks and months leading up to the American Revolution, these cells work through street protests, marches, and so on.

MINUTE MAN CELLS -- Cells in this network operate as a quick-reaction force, ready to rise on a moment's notice to punish aggression by the oppressor and to retaliate against atrocities by the goon squads.

F9 will soon be providing instructions on how your active cell can receive clandestine messages through the F9 Bulletin. If you have carefully thought through your cell's raison d'etre -- and arrived at a sense of direction and purpose -- you'll be better poised to make good use of the messages.

* * * B L O W B A C K

(Letters from readers. Blowback is spy-talk for unexpected backlash from covert ops. Readers' comments are edited for brevity and style.)

BLOWBACK ITEM #1 -- SANITIZING A HARD DISK

Our website article Uncrackable Email describes how to keep the FBI from reading your encrypted messages. A friend in military intelligence writes -- "The preferred method for sanitizing a hard disk is to remove the unit from the computer, disassemble it, take out the platters, and sand them with coarse-grit sandpaper."

BLOWBACK ITEM #2 -- SURVEILLANCE TACTICS

The same article, Uncrackable Email, also describes the various methods used by surveillance teams to watch you -- including surreptitious entry and the installation of miniature video cameras in the ceiling of your office. An F9 reader who has just finished serving time writes -- "I never would have believed it if it hadn't happened to me exactly the way your article describes it. The prosecutor introduced evidence from a video camera in the ceiling of my office."

* * * S I T R E P

SITREP ITEM #1 -- POLICE BRUTALITY

In support of Amnesty International's recent stinging indictment of systematic police brutality across the USA, we're announcing our first weekend workshops. Three sessions are scheduled for January 9th and 10th, covering surveillance, countermeasures, and resistance tradecraft for underground activists and urban guerrillas. An illustrated, printed manual is available separately.

The full Amnesty International report, covering police brutality and other human rights abuses against Americans by the US Government, can be found at http://www.rightsforall-usa/info/report/index.htm

More information about our tradecraft workshops can be found at our website http://www.spycounterspy.com

SITREP ITEM #2 -- RANDOM STOP AND SEARCH

An F9 reader has reported to us that police in Indianapolis are randomly stopping motorists on the freeway off-ramps. Apparently a number of people have been searched for no valid reason. Here at F9 we are concerned that this type of action is the thin edge of the wedge. It is common practise for the government bureaucrats to test their methods of tyranny and oppression on minorities first. As the general population becomes desensitized to the infringement of rights of these "non-citizens", the government then starts to implement its measures against the ordinary citizen. Simply put, our point is this -- minorities and poor whites have been subject to so-called "profile stops" by police for many years. Are the authorities now beginning to use the same Gestapo-tactics against all US citizens?

* * * P A R T I N G S H O T

To continue to receive F9 Bulletin by email, simply do nothing. To cancel your subscription, reply to this email with "Remove" in the subject line.

ANTISURVEILLANCE TIP: You should promptly suspend your subscription if you detect new surveillance. This will help you deceive the goons into thinking that you are just one of the sheep. Watch mindless TV programs and read mindless magazine articles for a while. The goons will soon lose interest and downgrade the surveillance. Vickie will gladly email you all the back issues when you renew your subscription to F9 Bulletin.

Questions, comments, and suggestions about F9 Bulletin can be sent to F9's membership manager Vickie Nickel at training@bc.sympatico.ca

The next issue will be out a week from now. You can expect more frank talk about countersurveillance, antisurveillance, underground urban activism, and tradecraft. If you want the plain, unvarnished truth about how all this stuff really operates, you're reading the right newsletter.

Cheers.

From your friends at http://www.spycounterspy.com

Lee, Vickie, Agent X, and our network of whistleblowers

* * * F 9 B U L L E T I N * * *
Spy school for the rest of us.

Volume 1 Number 5 Thursday, October 15th, 1998
A free publication from http://www.spycounterspy.com

* * * I N S I D E T H I S I S S U E

* * * D U T Y O R T R E A S O N ?

Consider this premise. As a citizen, it is your DUTY to defend America against insurrection. You MUST act.

Here is the line of reasoning that backs up this logic.

ITEM #1 -- The right to form a militia is guaranteed by the 2nd Amendment to the Constitution.

ITEM #2 -- The militia is "we the people"; the militia is NOT the government. According to the US Code, the militia consists of citizens between the ages of 17 and 45 (or 65 if you have prior military service).

ITEM #3 -- The militia is charged with defending America against ALL enemies, both foreign and domestic. According to the US Code, the militia MUST ACT in cases of invasion by foreign nations or ATTEMPTS BY INTERNAL LAWLESS ELEMENTS TO TAKE OVER AMERICA. Look around you. Does not this describe the current situation in the USA? By definition, an element attempting to subvert the Constitution is engaged in insurrection.

Simply stated, here is where this logic leads.

Point 1 -- YOU ARE IN THE MILITIA.

Point 2 -- THE MILITIA'S DUTY IS TO FIGHT INSURRECTION.

Point 3 -- IS THERE NOT AN ATTEMPT BY AN INTERNAL LAWLESS ELEMENT TO TAKE OVER AMERICA?

Point 4 -- IF SO, THEN IT IS YOUR PATRIOTIC DUTY TO ACT.

If not NOW, when? If not THIS, what? If not YOU, who?

The insurrection is already well advanced. It is foolhardy to openly confront the perpetrators. They have already taken over the security forces and the secret police for their own purposes.

What is needed instead is a covert campaign of resistance by we the people. Instead of being formed along military lines, today's new militia must be organized like an underground resistance movement. Secrecy is vital. The oppressor crushes any dissent instantly.

An F9 reader submitted the preceding argument to us. We have edited her remarks for style and brevity.

The reader further contends that any citizen choosing NOT to act is guilty of TREASON. Here at F9 we find her arguments compelling. How about you?

* * * C A L L F O R A C T I V E C E L L S

Let's take a moment and reflect on the following.

"Is life so dear, or peace so sweet, as to be purchased at the price of chains and slavery? ...I know not what course others may take; but as for me, give me liberty or give me death." -- Patrick Henry, 1775.

For many citizens, these are powerful words -- just as meaningful today for America as they were 220 years ago. The words ring out with emotion. They embody the desperation felt by people forced to live under a tyrant who claimed the right to rule their lives.

Now let's fast-forward from 1776 America to 1998 Amerika.

Stop. Think. Have you had enough of the brutality and unfairness yet? Are you weary of turning your other cheek to the gang of hoodlums that has suborned The Constitution for their own ends? Have you had enough of the incremental stripping away of rights and freedoms in police-state Amerika?

Like the heroes and heroines of the American Revolution, the time has come to look deep in our hearts. We the people must ask ourselves if it is time to answer the call to idealism and sacrifice.

Consider the following two questions.

Question #1 -- Do you love your country but fear your government?

Question #2 -- Should you become an active cell?

Answer one question and you've answered both.

Becoming an active cell means becoming an active tactical unit (ATU). It means becoming an urban guerrilla. It means leading a double life.

Becoming an active cell means engaging in covert actions. It means being on station to receive clandestine, encrypted messages from F9 Command.

Becoming an active cell means demonstrating your patriotism in a tangible, meaningful way. It means holding an unshakeable conviction in the principles of freedom and fairness that are embodied in The Constitution.

Becoming an active cell means you understand -- and you feel, truly feel in a profoundly emotional way -- what it means to be an American. You understand, and you are deeply moved by, the principles that the heroes and heroines of the American Revolution fought and died for.

Becoming an active cell means you are disgusted by the corrupt system of tyranny embodied in today's Amerika.

"Tyranny, like hell, is not easily conquered." -- Thomas Paine, 1776.

Becoming an active cell is not for wannabees. It's for people who are ready to make a difference.

Becoming an active cell is for people who want to put America back on track.

If all these words describe you, then you are invited to become an active cell in F9.

As a patriotic volunteer, here's what you can expect.

As an active cell, you will plan and carry out your own operations. You will decide what needs to be done -- then you will do it.

As an active cell, you will be on station at a prescribed time once a week to receive an encrypted message from F9 Command. What does this mean? It means being at your computer, online, surfing the web for a specified 10-minute period once a week. F9 Command will use special software to establish a direct computer-to-computer link with you, bypassing the normal email system. In real time, an encrypted message will be transmitted direct from F9 Command's computer to your computer. The software automatically handles the encryption and decryption of the ciphertext message. After a successful transmission, all you need to do is use a text editor (like Windows WordPad, for example), to read the plaintext message at your convenience.

This is what spies call a one-way radio link (OWRL). It's our way of informing and advising you, keeping you in touch with the strategic and tactical objectives of today's resistance movement in America. F9 has no way of knowing -- and we don't want to know -- if you act on the information you receive via OWRL. Remember, F9 doesn't issue orders; F9 merely informs.

To become an active cell you need to do two things.

STEP ONE -- Point your browser to http://www.hilgraeve.com and download the DropChute software. It's free. Be sure to download DropChute, not DropChute+. Keep the downloaded file (it's named dcsetup.exe) on your hard disk. Do NOT install the software yet.

STEP TWO -- After you've successfully downloaded DropChute, send an email message to F9 membership manager Vickie Nickel at training@bc.sympatico.ca identifying yourself as an active cell. Tell her your nom de guerre and your email address (ie the email address you'll be using to receive messages from F9 Command).

Vickie will email you instructions on how to configure the DropChute software. She'll also tell you how to set up your real-time OWRL with F9 Command.

Becoming an active cell is completely separate from being a subscriber to F9 Bulletin. Whether or not you become an active cell, you will still receive the F9 Bulletin each Thursday until the goons come for us an hour before dawn.

Here's what Alexis de Tocqueville said of the newly-emerged United States of America 150 years ago -- "America is great because America is good. When America ceases to be good, America will cease to be great."

Look around you, and draw your own conclusions.

NO FEAR. NO MERCY. NO LIMIT.

NO FEAR -- of the heavyhanded tactics of the authorities acting unlawfully.

NO MERCY -- for the oppressor, or for those who have sold us out.

NO LIMIT -- to our courage and resolve. Winners never quit, and quitters never win. In the end we shall prevail.

* * * B L O W B A C K

(Letters from readers. Blowback is spy-talk for unexpected backlash from covert ops. Readers' comments are edited for brevity and style.)

BLOWBACK ITEM #1 -- In response to our recent article about how to beat SWAT, a reader writes -- "Pick up a good scanner with a frequency counter. Get used to the regular chatter that goes on around you day in and day out. You'll soon be able to tell when there is something going on, and what frequency they are coordinating with. Frequency counters allow you to pick up nearby field transmissions and compile a list of new frequencies that are not published in any scanner list. Remember, no time is ever wasted doing recon."

BLOWBACK ITEM #2 -- In response to the same SWAT article, another reader writes the following about the crisis negotiating team (CNT) -- "The CNT team is devious. They will promise you something and not give it to you. If they say a car is outside, they're probably using it as a ploy to flashbang you. A flashbang concussion grenade produces a flash of light and a deafening noise that can stun you for up to five minutes."

BLOWBACK ITEM #3 -- In response to our SitRep report about random stops and searches of ordinary citizens by the Indianapolis police, a reader who took the trouble to research the deteriorating situation there writes -- "In a somewhat related story, Indianapolis Police Department officers are no longer allowed to moonlight as bouncers for bars and strip joints. A few years ago we had a problem with a downtown bar-fight that involved some drunken off-duty police officers. Go figure."

* * * S I T R E P

(Assorted items of interest. Sitrep is spy-talk for situation report.)

SITREP ITEM #1 -- Here at Spy & CounterSpy we have received a report about an urban guerrilla method that we find very interesting. Apparently the Provisional IRA has been teaching civilians how to resist incoming CS grenades. CS is a form of tear gas used by the British military (and also used by various police, SWAT, and military agencies in the USA).

The method involves using "a basin of vinegar". It seems that vinegar can be used to mitigate the choking effects of CS. The implications are profound -- especially if you're involved in a standoff with the authorities. Being able to withstand a CS attack would contribute to leveling the playing field between the oppressor and the oppressed.

We need further information. Do you dip a towel in the basin and then wrap the towel over your face? Do you drape the towel over your head while you lean over the basin and inhale the vinegar fumes? Do you immerse your face into the vinegar? Do you cup your hands and splash the vinegar onto your face?

How does it work, and how effective is it? If you have any inside information, please send email to F9 membership manager Vickie Nickel at training@bc.sympatico.ca

SITREP ITEM #2 -- Numerous readers responded to our request for assistance in locating a copy of MINI MANUAL OF THE URBAN GUERRILLA, by Carlos Marighella. If you'd like to have a look at the document, point your browser to http://www.trailerpark.com/phase2/lenflank/minimanl.htm

It has been reported to us that private security firms are using the Mini Manual during their consultations with corporate executives. It would appear that the corporate elite is afraid -- just like government is afraid -- of we the people.

SITREP ITEM #3 -- It has been reported to us that US lawmakers were ready last Thursday to approved a long-sought FBI proposal that would expand wiretapping capabilities. Law enforcement agencies would be allowed to tap any telephone used by or simply "near" a suspect. Such a blanket authoritization would mean the FBI would not require authoritization to tap specific telephones. The proposal was tabled during a closed-door meeting about the Intelligence Authorization Conference Report.

(EDITOR'S NOTE -- In the few days since the preceding paragraph was written, the legislation was approved during the final hours of the 105th Congress. The FBI and other goon squads now have the "right" to engage in "roving wiretaps". There's nothing between you and the goons. No permission from a judge is needed. It's strictly a "political" decision. This is what is called a TOTALITARIAN POLICE-STATE, folks. Welcome to Amerika 1998.)

* * * A S K A G E N T X

(Questions from readers recently received by F9.)

QUESTION -- "Have had some things happening with personal land-line telephone calls... clicks, noises, and a drop in ambient or background noise. I've also had mail opened before delivery. Otherwise, no pattern of foot surveillance or vehicle surveillance has been detected. Recommendations?"

AGENT X REPLIES -- Don't let them know you're on to them. Their next step is surreptitious entry. They'll attempt to get inside your office or home undetected. You can use misinformation to frustrate their efforts.

Here's how. Leave magazines laying around that imply you're interested in things that you're really not interested in. Put "sticky notes" on the refrigerator reminding yourself to watch TV programs (that you're really not interested in, of course). Simply stated, distribute various props around your office and home for the express purpose of throwing the goons off the scent. They're trying to build up a profile on you, so de-emphasize the interests that are important to you. And be sure to sanitize your trash. Don't put anything out with the trash that you don't want them being aware of, because they WILL snatch your garbage (it's called garbology -- and they usually learn a lot from it). Your overall goal, of course, is to fool them into thinking that you're just one of the sheeple. You wanna be like the adlib from the old rock'n'roll song, "Grrrrr... err, I mean Baa-aaa".

* * * P A R T I N G S H O T

To continue to receive F9 Bulletin by email, simply do nothing. To cancel your subscription, reply to this email with "Remove" or "Unsubscribe" in the subject line.

ANTISURVEILLANCE TIP: You should promptly suspend your subscription if you detect new surveillance. This will help you deceive the goons into thinking that you are just one of the sheep. Watch mindless TV programs and read mindless magazine articles for a while. The goons will soon lose interest and downgrade the surveillance. Vickie will gladly email you all the back issues when you renew your subscription to F9 Bulletin.

Questions, comments, and suggestions about F9 Bulletin can be sent to F9's membership manager Vickie Nickel at training@bc.sympatico.ca

The next issue will be out a week from now. You can expect more frank talk about countersurveillance, antisurveillance, underground urban activism, and tradecraft. If you want the plain, unvarnished truth about how all this stuff really operates, you're reading the right newsletter.

Cheers.

From your friends at http://www.spycounterspy.com

Lee, Vickie, Agent X, and our network of whistleblowers and contributors

* * * F 9 B U L L E T I N * * *
Spy school for the rest of us.

Volume 1 Number 6 Thursday, October 22nd, 1998
A free publication from http://www.spycounterspy.com

* * * I N S I D E T H I S I S S U E

* * * S U R V I V E A S T A N D O F F

They'll try a no-knock entry first, of course. And it usually works. Before you even realize what's happening, they kick in the door, dash into your bedroom, and slam the muzzle of a 9mm Heckler & Koch submachine gun up against your forehead.

But you're not one of the sheep. Your door is reinforced. And your return fire made the goons back off. Remember, to them it's just a paycheck. Think of them as bullies looking for victims. They usually run at the first sign of determined resistance.

Next comes the seige. They surround your house, cut off the electricity, toss over a throw-phone, and call in the crisis negotiation team to start lying to you.

In a barricade situation, your real adversary is time. Sure, the cops may have your house surrounded -- they may even have a couple of snipers on rooftops. But not much else is going to happen. Not unless they get inside. Or unless you go outside.

Your biggest problem is the CS grenades that they're going to lob through the windows. CS is tear gas. Chemical name orthochlorobenzalmalononitrile. Named after Corson and Stoughton, the developers.

CS is chemical warfare. Chemical agents. Incapacitating agents, they're called. CS falls into the subclass of lacrimators, which are tear-producing agents.

CS is an extremely potent form of tear gas. It's strong, persistant, and water soluable. It produces a burning sensation in all wet areas -- nose, eyes, nasal passages, bronchial passages, and lungs. Your body immediately begins producing huge quantities of mucous -- it's like an instant case of multiple pneumonia. All you can think of is the incredible pain. Burning, burning, burning. Your eyes are welded shut. Panic sets in. Disorientation. Fear. You gotta get out of here. You'll do anything to escape the pain.

Run outside and you're finished. They'll slam you down to the ground. Surround you and beat you senseless. Then cuff your hands behind you. And probably put you out with a standard police choke-hold. Or maybe they'll just let the German Shepherd dogs have a go at you first. (Standard "police dogs" simply rip at your wrists and ankles. Maybe slash up your hands and face a bit as you try to defend yourself. Hardened military "attack dogs" go straight for your groin and neck. It isn't pretty.)

But we digress. To get back to the main problem, your house is surrounded. Hmmm. If you don't have a pre-planned escape route or a hiding place, you are stuck. Your best option to to negotiate through a third-party. DO NOT EVER AGREE TO USE A POLICE-SUPPLIED NEGOTIATOR. They are too skilled at deception.

If you cannot escape, then you must NEGOTIATE YOUR WAY INTO CUSTODY, preferably in the presence of TV cameras. That's because the goons aren't focused on arresting you, they're waiting to execute you. So you gotta negotiate. But you can't negotiate if you're choking from the burning CS cannisters they just shot through the windows.

And that's what this article is about. How to survive the tear gas.

Technically, it's not really a gas at all. It is composed of microfine particles carried on the smoke produced by the grenade. The smoke is white -- in Britain they call it tear smoke -- here in the USA we call it tear gas.

There are four ways you can defend yourself against incoming CS grenades.

DEFENSE #1 -- SURPLUS GAS MASK ;-)

This is your best option. Available at most surplus stores. You can pick up a brand-new Israeli gas mask for $15 to $30. A used domestic mask with a brand-new filter cartridge runs about the same price. This is your best defense. Keep your mask near where you sleep. All the masks work the same way. One air passage for breathing in. Another passage for breathing out. This makes the filter cartridge last longer. An internal seal over your nose and mouth keeps your breath from fogging up the eye glasses. The filters are effective because the CS chemical is carried on the smoke particles. Filter out the smoke particles and you've filtered out the CS agent.

DEFENSE #2 -- INHIBIT THE LACRIMATING AGENT :-)

This is your next-best option. Use thick gloves or a doubled-up towel to pick up the grenade. It'll be hot. You'll get third-degree burns if you attempt to grab it with your bare hands. Immerse the grenade in vinegar. The IRA has taught Irish civilians to keep their kitchen sink or bathroom basin filled with vinegar when the British troops are doing a sweep of the neighborhood. That's because the Brits confiscate any gas masks they find, of course. Here's what you can do. Keep a couple containers of vinegar and a large bucket near where you sleep. As the situation unfolds, fill the bucket with vinegar. When a CS grenade is deployed, pick it up and drop it into the bucket. Here's another way to use the vinegar. In a pinch you can soak some towels in the vinegar and place the towels over your nose and mouth. This method ain't perfect, but it'll get you through the roughest moments. More tips. Vaseline on exposed skin will help protect you from the general irritation that CS produces. The PLO teaches Palestinian civilians to use onions to get the chemical agent off their exposed skin. Cut a raw onion in half and use it like a scrub brush.

DEFENSE #3 -- NEUTRALIZE THE LACRIMATING AGENT :-)

This is your third-best option. Instead of vinegar, keep a supply of chlorine bleach on hand. Chlorine bleach is sodium hypochlorite. It is easiest to store in its powdered form. Toss some into your bucket, add some water, and you've got chlorine bleach on demand. Using thick gloves or a folded rag, drop the burning grenade into the bucket. The bleach neutralizes the active chemical, rendering it ineffective.

DEFENSE #4 -- THROW IT BACK AT THEM >:-)
If the grenade has been incorrectly deployed, you may be able to pick it up and throw it back out the window. (Protect your hands!)

That's the good news. Here's the bad news.

What we've just finished describing is the burning-style munition. The grenade simply burns and generates smoke. The smoke carries the CS chemical agent.

The goons can also use blast-style munitions. The agent is delivered through one detonation. Without a gas mask, you've got a major problem.

The military can also deliver CS by spraying, including water cannon.

Like we said, it ain't a pretty scenario.

Recommendation? Go out this weekend and get yourself a surplus gas mask.

[Editor's Note -- Here at F9 we wish to express our heartfelt thanks to the many whistleblowers, agents-in-place, and experts who shared their technical knowledge with us. This article wouldn't have been possible without your help. You know who you are. On behalf of our readers, thank you.]

* * * S I T R E P

(Assorted items of interest. Sitrep is spy-talk for situation report.)

SITREP ITEM #1 -- CIA COVERT OPS
Government reports over the past 15 years paint a damning picture of CIA operations. One of every THREE covert operations involves rigging elections. So much for DEMOCRACY. One of every FOUR covert operations involves media propaganda. So much for FREEDOM OF THE PRESS. One of every FIVE covert operations involves arms sales. So much for NONPROLIFERATION. Even worse, the reports confirm that the CIA is not repeat NOT a rogue element. It is NOT out of control. On the contrary, starting with the 1975 Pike Committee report, various House committees have confirmed again and again that the CIA acted -- and continues to act -- under the DIRECT ORDERS of the goons in the White House.

SITREP ITEM #2 -- THE GREEN MAMBA
Here at F9 we have received confidential reports of a new computer security product being developed offshore by an American group of investors. Code-named The Green Mamba after the poisonous snake of the same name, the infrared-based hardware key is designed to protect notebook and laptop computers from the prying eyes of NSA, FBI, IRS, et al. It will also make your computer useless to any thief. You carry the key on your keyring with your house keys, car keys, and so on. Your portable computer will not boot unless the key is held within 18 inches of the machine's infrared port. All data on your hard drive is

kept encrypted when not in use, so even if the goons manage to bypass your infrared key, your information remains secure. Expect the product to hit the US market in about 8 months. We were offered further information and a beta version if we would sign a nondisclosure agreement. We declined.

SITREP ITEM #3 -- FEMA PLAYING ROUGH

According to one of our whistleblowers, FEMA has recently been offering to train SWAT teams in terrorist containment. Here at F9, we interpret "terrorist containment" to mean "operations against US citizens". If anyone has any further information on this ugly development, please email F9 membership manager Vickie Nickel at training@bc.sympatico.ca

* * * B L O W B A C K

(Letters from readers. Blowback is spy-talk for unexpected backlash from covert ops. Readers' comments are edited for brevity and style.)

BLOWBACK ITEM #1 -- BRITAIN

A frustrated F9 reader from Britain writes, "You guys think you have it hard. Well, consider this. The population here has been completely disarmed. Only the crooks and cops have weapons. We can't even own a slingshot here. The British are very, very effective at internal security. More than one per cent of the population are deployed as part of the security service."

BLOWBACK ITEM #2 -- USA

A curious F9 reader with an anonymous email account writes, "I would like to see an article about building security. I'm interested in outer, middle, and inner security -- as well as an explanation of how a man-trap works."

BLOWBACK ITEM #3 -- USA

A rehabilitated ex-spook writes, "You are doing a great service. I am retired from the US Army. I served as a counterintelligence special agent. My last assignment was counter-narcotics operations. What a waste... nothing more than an excuse for the authorities to trample on everyone's rights."

BLOWBACK ITEM #4 -- OFFSHORE

An F9 reader from overseas writes, "You may want to check out Kill Or Get Killed by Rex Applegate, from Paladin Press. Also note that the Mini Manual for the Urban Guerrilla has been banned here in [deleted] since the 1960s." [Editor's Note -- In the interests of safety, we deleted the name of the country to protect the identity of our reader.]

BLOWBACK ITEM #5 -- USA

A rehabilitated ex-cop writes, "Your website has taught me more over the past 25 hours that I've been reading it than all the specialized training I received in law enforcement over a 27-year career."

BLOWBACK ITEM #6 -- USA

Another ex-cop writes, "I worked in law enforcement for nearly 30 years. To date I've found nothing to compare with your website. Not only is it accurate, but it's of the utmost importance for the lay person.

Anyone who will take the time to read and study your material stands a better chance of avoiding being victimized by the system."

BLOWBACK ITEM #7 -- USA
A cryptography buff writes, "Your website makes no mention of steganography. I have several programs that can hide text files inside an audio file or inside an image file. The process does not noticeably degrade the quality of the original audio or image. I would have thought that this concealed method of cryptography would be very useful, because anyone using typical encryption would arouse the suspicion of the authorities. I can provide these steganography programs if you are interested."

* * * C A L L F O R A S S I S T A N C E

F9 needs your help.

As you probably already know, we're forming up networks of active cells. We've run into a snag with our communications strategy. Here's the story so far.

We originally intended to use PGP to send encrypted messages to our active tactical units (active cells). However, the idiosyncracies between different versions of PGP made this impractical. Incompatibilities between encryption algorithms, key lengths, key exchange protocols, signing protocols, ciphertext header anomolies, and operating system inconsistencies (Windows vs. DOS) made the process simply too labor intensive. In addition, we were concerned that recent Windows versions of PGP apparently no longer use the open source code model. If you want to test it yourself, PGP is available at http://web.mit.edu.network/pgp.html

Next we looked at RPK InvisiMail, which handled all the key exhanging and encryption/decryption automatically. RPK was developed offshore, away from the prying eyes of NSA et al, so we liked the security. Open algorithm. No trap doors. However, we encountered two problems. First, if the recipient wasn't using InvisiMail, the sender's software would simply send the message as plaintext. This could have very serious ramifications if the sender were relying on an encrypted transmission. Second, while we were testing the software, we encountered some instability during the handshaking between two users. The recipient's computer froze a few times. If you want to test it yourself, RPK InvisiMail is available at http://www.invisimail.com

Then we looked at DropChute. We liked what we saw. The software bypassed the normal email protocol, which is sloppy and inconsistent. Often 4 or 5 copies of your original message are send to different servers, where they are never erased. DropChute, on the other, establishes a direct link in real time between the sender's computer and the recipient's computer. One message, one connection, one transmission, one confirmation, all automatically encrypted. However, we've just begun to encounter a few problems. DropChute apparently doesn't work with some of the new high-speed cable modems. Further, DropChute requires Windows 95/98/NT -- it isn't available for OS/2 or DOS or Macs. And DropChute requires that both the sender and the recipient be at their computers -- and it doesn't seem to work with anonymous email accounts that are Web-based instead of ISP modem-based. If you want to test it yourself, DropChute is available at http://www.hilgraeve.com

---

That's why we need your help. Is there an efficient way to communicate with our active cells (and perhaps with F9 subscribers)?

Here are our criteria...

F9 needs a method that will reach as many readers as possible, including those using MS DOS, Windows 3.1, Windows 95, Windows 98, Windows NT, IBM OS/2, Linux, Macs, and others.

F9 needs a method that will keep messages confidential from nosy busybodies. Some readers are at computers that aren't secure from over-the-shoulder lookieloos.

F9 needs a method that makes it necessary for the authorities to deliberately place a targeted individual under surveillance before they can begin to intercept and crack his/her email messages. This increases the chances that you'll spot the surveillance team setting up. We would prefer not repeat NOT to use any method that makes it easy for the authorities to troll for F9 readers by intercepting email messages at random.

F9 needs a method that will permit readers to take advantage of the firewall security described in our website tutorial about keeping the FBI out of your email. (To read the tutorial go to our home page at http://www.spycounterspy.com and click on Uncrackable Email.)

And, lastly, we're hoping to find an email method that will work with our bulk emailer software, GroupMail. To test this software yourself, you can download a free trial copy from http://www.firebird.net

---

We still hope to be able to use DropChute with readers who are able to run it. And we're prepared to use plaintext email if we have to. After all, when all is said and done, it is completely lawful for you to read the email we'll be sending you -- especially in the context of the elliptical conversation tradecraft that we'll be using -- and teaching you -- in coming issues of F9.

But is there a more effective way for us to communicate with you over the Web?

If you've got some ideas, please send email to F9 membership manager, Vickie Nickel :-) at training@bc.sympatico.ca

For example, if you've got a custom build of PGP, we'd be glad to evaluate it. A PGP-like program with an extensible front end for different operating systems, complete with shredding capabilities... are we asking too much? Or if you know of offshore software, please give us a buzz ;-) Or if you can think of a combination of programs that might do the trick... please email us.

* * * A S K A G E N T X

(Questions from readers.)

This reader's question concerns our one-time pad tutorial at the Spy & CounterSpy website.

QUESTION --
"Why not use a Beale code instead of the one-time pad? The key could be anything -- a local newspaper, a telephone directory, or a copy of a book like War and Peace. I really don't get the use of a one-time pad. It seems to present problems, i.e. getting the key distributed to the appropriate people."

AGENT X REPLIES --
The randomness of the key is vital. The security of the one-time pad relies on two factors. First, the key must be random. Second, the key can used only once. If the key isn't truly random -- or if you use a key more than once -- the cryptanalysts at NSA will crack your ciphertext.

Here's a case study that shows how serious this is.

During the Second World War, the Russians ran a group of espionage agents in Britain. These top-producing agents, called "The Cambridge Five", included Kim Philby, Donald Maclean, Guy Burgess, Anthony Blunt, and John Cairncross.

The KGB was using a one-time pad system to send telegrams to Moscow from its field offices in Britain and the United States. Britain's MI.5 was completely in the dark. Hoover's FBI was busy chasing Nazis.

Then in 1951 things started going horribly wrong for the Russians. Master spy Kim Philby, who had wormed his way deep into the British intelligence establishment, learned that American cryptanalyst Meredith Gardner had discovered a blunder in a telegram sent from New York to Moscow. In 1942 a Russian cipher clerk in the Washington embassy had exhausted his supply of one-time pads. The diplomatic pouch containing the new pads had been delayed because the ship's captain decided to postpone the Atlantic crossing because of intense German submarine activity.

The cipher clerk used the SAME one-time pad for two messages.

Seven years later in 1949, an American mathematics whiz named Meredith Gardner was able to crack the two messages. The effort was called Project Venona.

The result? Russian spy-handler Yuri Modin watched in horror as his network of top agents fell apart. By 1951 the FBI and MI.5 had unearthed enough clues to reveal the identity of one of the Cambridge Five -- agent Homer (Donald Maclean). The dominoes began to fall. Eventually even the grandmaster himself, Kim Philby, was implicated.

The Russians shot the cipher clerk.

The lesson? A one-time pad is foolproof only if it is RANDOM -- and only if it's used JUST ONCE. If there is ANY PATTERN AT ALL, then the goons will be able to crack your messages. Don't make the same
mistake the Russian cipher clerk made in 1942.

Nobody ever said that using a one-time pad was easy. It involves nitpicking work to generate a random key. It is inconvenient to distribute the one-time pads to your correspondents.

But the one-time pad is the only cryptography system that will keep you out of the internment camps. The one-time pad is the ONLY system that cannot be broken -- either in practise or in theory. Period.

Besides, when the goons kick in the reader's door an hour before dawn, he's going to find it a lot easier to swallow a one-time pad than a copy of the daily newspaper.

* * * P A R T I N G S H O T

ANTISURVEILLANCE TIP: You should promptly suspend your subscription if you detect new surveillance. This will help you deceive the goons into thinking that you are just one of the sheep. Watch mindless TV programs and read mindless magazine articles for a while. The goons will soon lose interest

and downgrade the surveillance. Vickie will gladly email you all the back issues when you renew your subscription to F9 Bulletin.

The next issue will be out a week from now. You can expect more frank talk about countersurveillance, antisurveillance, underground urban activism, and tradecraft. If you want the plain, unvarnished truth about how all this stuff really operates, you're reading the right newsletter.

Cheers.

From your friends at http://www.spycounterspy.com

Lee, Vickie, Agent X, and our network of whistleblowers and contributors

* * * F 9 B U L L E T I N * * *

Volume 1 Number 7 Thursday, October 29th, 1998
A free publication from http://www.spycounterspy.com

* * * I N S I D E T H I S I S S U E

* * * C E L L S E C U R I T Y

A cell is an active tactical unit. A cell is usually formed of three or four people. But a cell can also be just one person. Or it can be nine or ten people.

A cell is a covert unit. It is a secret unit. A cell can plan and carry out operations only if the cell remains unknown to the authorities.

The existence of the cell must remain secret. The purpose and goals of the cell must remain secret. The identities of the cell members must remain secret.

A cell is a conspiratorial organization.

As a cell member, you must lead a double life. This means you must lead a public life and you must also lead a secret life. For your public life, you must adopt a persona that allows you to live openly in the general population. For your secret life, you must adopt a nom de guerre that allows you to remain unknown to the general population and to the authorities.

Here is an example. Suppose your real name is "John Doe". When you join an active cell, you might perhaps adopt the nom de guerre of "Alpha".

Whenever you engage in covert activities, you are Alpha. You communicate ONLY with other members of your cell.

Whenever you are NOT engaged in covert activities, you are John Doe. John Doe is a model citizen in the eyes of the authorities. John Doe obeys all the rules. John Doe never does anything unlawful.

As John Doe, you can go shopping, get your hair cut, see a movie, go to work. You can do a lot of things, but you NEVER engage in covert activities as John Doe.

This firewall between your public life and your secret life must be maintained always. John Doe is your cover. You must never compromise the security of your cover.

Your cell, however, will need to communicate with the outside world. Your cell may need to contact other underground elements, issue statements to the news media, send communiques to the authorities, recruit new members, protect persecuted persons, and so on.

Suppose, for example, that your cell wishes to acquire weapons for self-defense during covert operations. [EDITOR'S NOTE -- This is merely an example, not a recommendation.]

The weapons cannot be purchased by John Doe. He must be protected from the possibility that the weapons may be used illegally. Having his identity linked with the weapons could eventually lead to his arrest and interrogation.

Nor can the weapons be purchased by Alpha. The cell must be protected from the possibility that the arms dealer is an undercover FBI agent -- or an informant. Even a well-intentioned arms dealer might eventually
be arrested and tortured to reveal the identities of his customers.

To preserve security, Alpha must use a "cut-out". Simply stated, the cell must use a "go-between" in its dealings with other underground elements.

A go-between is a person who knows only Alpha. The go-between does not know the identities of other members of the cell.

Suppose that the cell uses a go-between to purchase the weapons from an arms dealer on the black market. If the arms dealer is interrogated and tortured by the police, he can identify only the go-between. Alpha is safe.

Or is he?

After interrogating the arms dealer, the police will go out and pick up the go-between. Properly tortured, the go-between will incriminate Alpha. The cell has been fatally compromised.

Is there a better way to use cut-outs? Yes, there is.

At a secret meeting of the cell, it is agreed to acquire weapons for self-defense during covert operations. Alpha, the cell leader, is designated to make the purchase.

Alpha gets in touch with a go-between, Beta, who does not know any of the other members of the cell. Alpha gives his instructions to Beta.

The first go-between (Beta) gets in touch with a second go-between, Charlie.

It is the second go-between (Charlie), who makes the purchase from the arms dealer.

The first go-between (Beta), AFTER CAREFULLY CHECKING FOR SURVEILLANCE, accepts the weapons from the second go-between (Charlie). This transfer can be accomplished through a face-to-face meeting, through a dead-letter box, or through a brush pass.

Beta now has the weapons in his possession. Beta sets up a rendezvous with Alpha, the cell leader. AFTER METICULOUSLY CHECKING FOR SURVEILLANCE, Alpha accepts the weapons from Beta.

This double cut-out system will protect the members of the cell. Here's why.

Suppose that something goes wrong with the weapons purchase. It doesn't really matter what the problem is. The arms dealer might be an informant. Or he might be an undercover BATF agent. The arms dealer might be under surveillance by the FBI. Or a former customer of the arms dealer might have provided his name to the police.

No matter what goes wrong, a double cut-out will provide a margin of safety for the cell. Let's assume the arms dealer has been arrested. You must presume that he will talk. Here are two possible scenarios.

NASTY SCENARIO #1 -- CHARLIE IS UNDER SURVEILLANCE.
The arms dealer has been arrested. During interrogation he has named Charlie. The goons now have Charlie under surveillance. Remember, Charlie is the second go-between. He knows both Beta and the arms dealer. But Beta is practising good security. He is using the "drycleaning" method described at http://www.spycounterspy.com. [EDITOR'S NOTE -- Click on "Arrange secret meetings" to read the tutorial.] Here's what happens. Before meeting with Charlie, Beta observes that Charlie is under surveillance. Beta aborts the meeting. BETA BREAKS OFF ALL CONTACT WITH CHARLIE. The surveillance team never sees Beta and Charlie together. The cell's security is still intact. AS A PRECAUTION AGAINST CHARLIE'S EVENTUAL ARREST, the cell will arrange for Beta to go into hiding. Even if Charlie talks, the authorities will not be able to find Beta. And only Beta knows who Alpha is. The cell is safe.

NASTY SCENARIO #2 -- CHARLIE HAS BEEN ARRESTED.
The arms dealer has been arrested. During interrogation he has named Charlie. The goons have arrested Charlie. Remember, Charlie is the second go-between. He knows both Beta and the arms the dealer. Under normal circumstances, Beta will detect Charlie's SUDDEN DISAPPEARANCE. As soon as he finds out what has happened, Beta reports the problem to Alpha. In turn, Alpha gets in touch with other elements in the resistance movement who will ARRANGE FOR BETA TO GO INTO HIDING. No matter how long the police torture Charlie, the only name they can get out of him is Beta. But Beta has disappeared. And only Beta knows Alpha. So your cell's security remains intact. You can continue to plan and carry out operations.

Simply stated, the double cut-out method is the only way to protect the cell from the authorities. A single cut-out is good, but only a double cut-out can provide the margin of protection that is required in today's world. You need the extra buffer that the second go-between provides.

The lesson? Whenever part of the chain is compromised, the resistance movement must break the chain completely.

This means removing a link from the chain. There is no other way.

* * * B L O W B A C K

(Letters from readers. Blowback is spy-talk for unexpected backlash from covert ops. Readers' comments are edited for brevity and style.)

BLOWBACK ITEM #1 -- CONCEALED UZIs.
An ex-cop writes, "I was a police officer for twenty years and part of an anti-terrorist team. We worked closely with the security of El Al Airlines. That means Mossad. They carry black attache cases. When they jerk up on the handle the attache case falls away, leaving only a cocked Uzi submachine gun."

BLOWBACK ITEM #2 -- FEMA SIEGE.
In response to our SitRep article about FEMA offering to train SWAT teams in terrorist containment, a concerned F9 reader writes, "I believe that FEMA is training SWAT to be ready to search an entire city in the event of a terrorist attack. FEMA's first step will be to seal off the city."

BLOWBACK ITEM #3 -- FEMA LISTS.
Another F9 reader writes, "I heard somewhere that FEMA keeps a list of names of subversives for the purpose of rounding them up during a declared national emergency. If this is true, then the Y2K problem takes on a new dimension, especially if power outages and other disruptions begin to happen as predicted."

BLOWBACK ITEM #4 -- NEVER CONFESS.
Another ex-cop writes, "When dealing with any government agent, never never NEVER admit to anything under any circumstances. If you do, you will lose, big time. The goons love to play the goodguy-badguy routine. They will lie lie LIE to get what they want from you. Then they'll double-cross you. When the laundry is done, you'll be the one hung out to dry, because their lies will hold up in Court. The one thing I advise all my F9 friends is to never never NEVER confess -- and never never NEVER admit to anything. NOT EVEN TO MAKE A DEAL. Take it from me, an ex-cop who's been there."

BLOWBACK ITEM #5 -- BUGGED THROW-PHONES
In response to our article about beating SWAT, a former hostage-negotiator writes, "You can expect that every throw-phone being used today contains a hidden microphone. It will be transmitting to the negotiators. They can hear everything in the room. It's a helluva negotiation tool... cut the wires and only connect when the police negotiator wants to."

* * * S I T R E P

(Assorted items of interest. Sitrep is spy-talk for situation report.)

SITREP ITEM #1 -- BAD COPS.
These are the government's own statistics. A big-city police chief can expect to have the following officers arrested during a 12-month period -- 10 abuse of authority; 5 felony; 7 misdemeanour; 3 theft; 4 domestic violence. If these statistics don't show up in YOUR city, you've got to ask yourself if the police chief isn't covering up for his bad cops. That means the whole barrel is rotten, not just a few apples.

SITREP ITEM #2 -- VIOLENT CRIME IS UP.
Worried Americans are watching Australia. According to a recent story in the Brisbane Courier Mail, violent crime in that country has increased AS A RESULT OF MANDATORY HANDGUN REGISTRATION. Robberies involving guns rose 39% last year. THE BLACK MARKET IN GUNS IS BOOMING. Even law-abiding citizens are buying. The police are trotting out all kinds of excuses to try and explain away the problem. At the root of everything, of course, is the intention of the authorities to disarm the population -- and the peoples' fear of the government. Here in the USA, concerned citizens are predicting that violent crime will soar when mandatory gun registration is imposed by the US government in response to the Y2K problem.

SITREP ITEM #3 -- PROPAGANDA PRIMER.
The Spy & CounterSpy website doesn't yet contain any tutorials about propaganda. There are a number of good Internet sources for information. If you're interested in this black art, you might want to check out http://carmen.artsci.washington.edu/propaganda/contents.htm [EDITOR'S NOTE -- Our thanks to the F9 reader who passed us this tip.]

SITREP ITEM #4 -- DEPLETED URANIUM BULLETS.
During the Gulf War, coalition forces used rounds made of depleted uranium to penetrate the armor of Saddam's tanks. Can't quite picture it? Think of a hot knife through butter. In response to our recent article about beating SWAT, F9 Bulletin was contacted by a member of [deleted]'s military. He says that a depleted uranium round will penetrate SWAT's body armor. Then he goes on to name and describe some of his nation's military handgun ammunition. Here at F9 we're wondering if that wasn't his way of leaking that 9mm depleted uranium handgun ammunition is available. If anyone has any further information on this, please send email to F9 membership manager Vickie Nickel at training@bc.sympatico.ca [EDITOR'S NOTE -- The name of the country has been deleted to protect the identity of our reader.]

* * * M E S S A G E T O A C T I V E C E L L S

PLEASE STAND BY. FINAL ADJUSTMENTS TO MESSAGING SYSTEM. ENSURES SECURE VS NSA ATTACK. EXPECT CONTACT IN DUE COURSE. FIRST MESSAGE COMMUNICATIONS TEST ONLY. UNTIL THEN DO NOTHING TO JEOPARDIZE SELF. KEEP FAITH. WE SHALL PREVAIL AGAINST FORCES OF TYRANNY. CHEERS GEORGE WASHINGTON.

* * * P A R T I N G S H O T

ANTISURVEILLANCE TIP: You should promptly suspend your subscription if you detect new surveillance. This will help you deceive the goons into thinking that you are just one of the sheep. Watch mindless TV programs and read mindless magazine articles for a while. The goons will soon lose interest and downgrade the surveillance. Vickie will gladly email you all the back issues when you renew your subscription to F9 Bulletin.

Cheers.

From your friends at http://www.spycounterspy.com

Lee, Vickie, Agent X, and our network of whistleblowers and contributors

Mini-manual of the Urban Guerrilla

by Carlos Marighella

A Definition of the Urban Guerrilla

The chronic structural crisis characteristic of Brazil today, and its resultant political instability, are what have brought about the upsurge of revolutionary war in the country. The revolutionary war manifests itself in the form of urban guerrilla warfare, psychological warfare, or rural guerrilla warfare. Urban guerrilla warfare or psychological warfare in the city depends on the urban guerrilla.

The urban guerrilla is a man who fights the military dictatorship with arms, using unconventional methods. A political revolutionary and ardent patriot, he is a fighter for his country's liberation, a friend of the people and of freedom. The area in which the urban guerrilla acts is in the large Brazilian cities. There are also bandits, commonly known as outlaws, who work in the big cities. Many times assaults by outlaws are taken as actions by urban guerrillas.

The urban guerrilla, however, differs radically from the outlaw. The outlaw benefits personally from the action, and attacks indiscriminately without distinguishing between the exploited and the exploiters, which is why there are so many ordinary men and women among his victims. The urban guerrilla follows a political goal and only attacks the government, the big capitalists, and the foreign imperialists, particularly North Americans.

Another element as prejudicial as the outlaw and also operating in the urban area is the right-wing counterrevolutionary who creates confusion, assaults banks, hurls bombs, kidnaps, assassinates, and commits the worst imaginable crimes against the urban guerrillas, revolutionary priests, students, and citizens who oppose fascism and seek liberty.

The urban guerrilla is an implacable enemy of the government and systematically inflicts damage on the authorities and on the men who dominate the country and exercise power. The principal task of the urban guerrilla is to distract, to wear out, to demoralize the militarists, the military dictatorship and its repressive forces , and also to attack and destroy the wealth and property of the North Americans, the foreign managers, and the Brazilian upper class.

The urban guerrilla is not afraid of dismantling and destroying the present Brazilian economic, political, and social system, for his aim is to help the rural guerrillas and to collaborate in the creation of a totally new and revolutionary social and political structure with the armed people in power.

The urban guerrilla must have a certain minimal political understanding. To gain that he must read certain printed or mimeographed works such as:

Guerrilla Warfare by Che Guevara
Memories of a Terrorist
Some Questions about the Brazilian Guerrilla Operations and Tactics
On Strategic Problems and Principles
Certain Tactical Principles for Comrades Undertaking Guerrilla Operations

Organizational Questions
O Guerrilheiro, newspaper of the Brazilian revolutionary groups.

Personal Qualities of the Urban Guerrilla

The urban guerrilla is characterized by his bravely and decisive nature. He must be a good tactician and a good shot. The urban guerrilla must be a person of great astuteness to compensate for the fact that he is not sufficiently strong in arms, ammunition, and equipment.

The career militarists or the government police may have modern arms and transport, and can go about anywhere freely, using the force of their power. The urban guerrilla does not have such resources at his disposal and leads to a clandestine existence. Sometimes he is a convicted person or is out on parole, and is obliged to use false documents.

Nevertheless, the urban guerrilla has a certain advantage over the conventional military or the police. It is that, while the military and the police act on behalf of the enemy, whom the people hate, the urban guerrilla defends a just cause, which is the people's cause.

The urban guerrilla's arms are inferior to the enemy's, but from a moral point of view, the urban guerrilla has an undeniable superiority.

The moral superiority is what sustains the urban guerrilla.. Thanks to it, the urban guerrilla can accomplish his principal duty, which is to attack and to survive.

The urban guerrilla has to capture or divert arms away from the enemy to be able to fight. Because his arms are not uniform, since what he has are expropriated or have fallen into his hands in different ways, the urban guerrilla faces the problem of a variety of arms and a shortage of ammunition. Moreover, he has no place to practice shooting and marksmanship.

These difficulties have to be surmounted, forcing the urban guerrilla to be imaginative and creative, qualities without which it would be impossible for him to carry out his role as a revolutionary.

The urban guerrilla must possess initiative, mobility, and flexibility, as well as versatility and a command of any situation. Initiative especially is an indispensable quality. It is not always possible to foresee everything, and the urban guerrilla cannot let himself become confused, or wait for orders. His duty is to act, to find adequate solutions for each problem he faces, and not to retreat. It is better to err acting than to do nothing for fear of erring. Without initiative there is no urban guerrilla warfare.

Other important qualities in the urban guerrilla are the following: to be a good walker, to be able to stand up against fatigue, hunger, rain, heat. To know how to hid and to be vigilant. To conquer the art of dissembling. Never to fear danger. To behave the same by day as by night. Not to act impetuously. To have unlimited patience. To remain calm and cool in the worst conditions and situations. Never to leave a track or trail. Not to get discouraged.

In the face of the almost surmountable difficulties of urban warfare, sometimes comrades weaken, leave, give up the work.

The urban guerrilla is not a businessman in a commercial firm nor is he a character in a play. Urban

guerrilla warfare, like rural guerrilla warfare, is a pledge the guerrilla makes to himself. When he cannot face the difficulties, or knows that he lacks the patience to wait, then it is better to relinquish his role before he betrays his pledge, for he clearly lacks the basic qualities necessary to be a guerrilla.

How the Urban Guerrilla Lives and Subsists

The urban guerrilla must know how to live among the people and must be careful not to appear strange and separated from ordinary city life.

He should not wear clothes that are different from those that other people wear. Elaborate and high fashion clothing for men or women may often be a handicap if the urban guerrilla's mission takes him into working class neighborhoods or sections where such dress is uncommon.

The same care has to be taken if the urban guerrilla moves from the South to the North or vice versa.

The urban guerrilla must live by his work or professional activity. If he is known and sought by the police, if he is convicted or is on parole, he must undergo and sometimes must live hidden. Under such circumstances, the urban guerrilla cannot reveal his activity to anyone, since that is always and only the responsibility of the revolutionary organization in which he is participating.

The urban guerrilla must have a great capacity for observation, must be well informed about everything, principally about the enemy's movements, and must be very searching and knowledgeable about the area in which he lives, operates, or through which he moves.

But the fundamental and decisive characteristic of the urban guerrilla is that he is a man who fights with arms; given this condition, there is very little likelihood that he will be able to follow his normal profession for ling without being identified. The role pf expropriation thus looms as clear as high noon. It is impossible for the urban guerrilla to exist and survive without fighting to expropriate.

Thus, within the framework of the class struggle, as it inevitably and necessarily sharpens, the armed struggle of the urban guerrilla points toward two essential objectives:

a) the physical liquidation of the chiefs and assistants of the armed forces and of the police;

b) the expropriation of the government resources and those belonging to the big capitalists, latifundists, and imperialists, with small expropriations used for the maintenance of individual urban guerrillas and large ones for the sustenance of the revolution itself.

It is clear that the armed struggle of the urban guerrilla also has other objectives. But here we are referring to the two basic objectives, above all expropriation. It is necessary for every urban guerrilla to keep in mind always that he can only maintain his existence if he is disposed to kill the police and those dedicated to repression, and if he is determined--truly determined--to expropriate the wealth of the big capitalists, the latifundists, and the imperialists.

One of the fundamental characteristics of the Brazilian revolution is that from the beginning it developed around the expropriation of the wealth of the major bourgeois, imperialists, and latifundists

interests, without excluding the richest and most powerful commercial elements engaged in the import-export business.

And by expropriating the wealth of the principal enemies of the people, the Brazilian revolution was able to hit them at their vital center, with preferential and systematic attacks on the bank network--that is to say, the most telling blows were leveled against capitalism's nerve system.

The bank robberies carried out by the Brazilian urban guerrillas hurt such big capitalists as Moreira Salles and others, the foreign firms which insure and reinsure the banking capital, the imperialist companies, the federal and state governments--all of the systematically expropriated as of now.

The fruit of these expropriations has been devoted to the work of learning and perfecting urban guerrilla techniques, the purchase, the production, and the transportation of arms and ammunition for the rural areas, the security apparatus of the revolutionaries, the daily maintenance of the fighters, of those who have been liberated from prison by armed force and those who are wounded or persecuted by the police, or to any kind of problem concerning comrades liberated from jail, or assassinated by the police and the military dictatorship.

The tremendous costs of the revolutionary war must fall on the big capitalists, on imperialism, and the latifundists and on the government, too, both federal and state, since they are all exploiters and oppressors of the people.

Men of the government, agents of the dictatorship and of North American imperialism principally, must pay with their lives for the crimes committed against the Brazilian people.

In Brazil, the number of violent actions carried out by urban guerrillas, including deaths, explosions, seizures of arms, ammunition, and explosives, assaults on banks and prisons, etc., is significant enough to leave no room for the doubt as to the actual aims of revolutionaries. The execution of the CIA spy Charles Chandler, a member of the U.S. Army who came from the war in Viet-Nam to infiltrate the Brazilian student movement, the military henchmen killed in bloody encounters with urban guerrillas, all are witnesses to the fact that we are in full revolutionary war and that the war can be waged only by violent means.

This is the reason why the urban guerrilla uses armed struggle and why he continues to concentrate his activity on the on the physical extermination of the agents of repression, and to dedicate twenty-four hours a day to expropriation from the people's exploiters.

Technical Preparation of the Urban Guerrilla

No one can become an urban guerrilla without paying special attention to preparation.

The technical preparation of the urban guerrilla runs from the concern for his physical preparedness, to knowledge of and apprenticeships in professions and skills of all kinds, particularly manual skills.

The urban guerrilla can have strong physical resistance only if he trains systematically. He cannot be a good fighter if he has not learned the art of fighting. For that reason the urban guerrilla must learn and

practice various kinds of fighting, of attack and personal defense.

Other useful forms of physical preparation are hiking, camping, and practice in survival in the woods, mountain climbing, rowing, swimming, skin diving, training as a frogman, fishing, harpooning, and the hunting of birds, small and big game.

It is very important to learn how to drive, pilot a plane, handle a motor boat and a sail boat, understand mechanics, radio, telephone, electricity, and have some knowledge of electronic techniques.

It is also important to have a knowledge of topographical information, to be able to locate one's position by instruments or other available resources, to calculate distances, make maps and plans, draw to scale, make timings, work with an angle protractor, a compass, etc.

A knowledge of chemistry and of color combination, of stamp making, the domination of the technique of calligraphy and the copying of letters and other skills are part of the technical preparation of the urban guerrilla, who is obliged to falsify documents in order to live within a society that he seeks to destroy.

In the area of auxiliary medicine he has the special role of being a doctor or understanding medicine, nursing, pharmacology, drugs, elemental surgery, and emergency first aid.

The basic question in the technical preparation of the urban guerrilla is nevertheless to know how to handle arms such as the machine gun, revolver, automatic, FAL, various types of shotguns, carbines, mortars, bazookas, etc.

A knowledge of various types of ammunition and explosives is another aspect to consider. Among the explosives, dynamite must be well understood. The use of incendiary bombs, of smoke bombs, and other types are indispensable prior knowledge.

To know how to make and repair arms, prepare Molotov cocktails, grenades, mines, homemade destructive devices, how to blow up bridges, tear up and put out of service rails and sleepers, these are requisites in he technical preparation of the urban guerrilla that can never be considered unimportant.

The highest level of preparation for the urban guerrilla is the center for technical training. But only the guerrilla who has already passed the preliminary examination can go to this school--that is to say, one who has passed the proof of fire in revolutionary action, in actual combat against the enemy.

The Urban Guerrilla's Arms

The urban guerrilla's arms are light arms, easily exchanged usually captured from the enemy, purchased, or made on the spot.

Light arms have the advantage of fast handling and easy transport. In general, light arms are characterized as short barreled. This includes many automatic arms.

Automatic and semiautomatic arms considerably increase the fighting power of the urban guerrilla. The disadvantage of this type of arm for us is the difficulty in controlling it, resulting in wasted rounds or in a prodigious use of ammunition, compensated for only by optional aim and firing precision. Men who are poorly trained convert automatic weapons into an ammunition drain.

Experience has shown that the basic arm of the urban guerrilla is the light machine gun. This arm, in addition to be efficient and easy tp shoot in an urban area, has the advantage of being greatly respected by the enemy. The guerrilla must know thoroughly how to handle the machine gun, now so popular and indispensable to the Brazilian urban guerrilla.

The ideal machine gun for the urban guerrilla is the Ina 45 caliber. Other types of machine guns with different calibers can be used--understanding, of course, the problem of ammunition. Thus it is preferable that the industrial potential of the urban guerrilla prevent the production of a single machine gun so that the ammunition used can be standardized.

Each firing group of urban guerrillas must have a machine gun managed by a good marksman. The other components of the group must be armed with .38 revolvers, our standard arm. The .32 is also useful for those who want to participate. But the .38 is preferable since its impact usually puts the enemy out of action.

Hand grenades and conventional smoke bombs can be considered light arms, with defensive power for cover and withdrawal.

Long barrel arms are more difficult for the urban guerrilla to transport and attract much attention because of their size. Among the long barrel arms are the FAL, the Mauser guns or rifles, hunting guns such as the Winchester, and others.

Shotguns can be useful if used at close range and point blank. They are useful even for a poor shot, especially at night when precision isn't much help. A pressure airgun can be useful for training in marksmanship. Bazookas and mortars can also be used in action but the conditions for using them have to be prepared and the people who use them must be trained.

The urban guerrilla should not try to base his actions on the use of heavy arms, which have major drawbacks in a type of fighting that demands lightweight weapons to insure mobility and speed.

Homemade weapons are often as efficient as the best arms produced in conventional factories, and even a cut-off shotgun is a good arm for the urban guerrilla.

The urban guerrilla's role as gunsmith has a fundamental importance. As gunsmith he takes care of the arms, knows how to repair them, and in many cases can set up a small shop for improvising and producing efficient small arms.

Work in metallurgy and on the mechanical lathe are basic skills the urban guerrilla should incorporate into his industrial planning, which is the construction of homemade weapons.

This construction and courses in explosives and sabotage must be organized. The primary materials for practice in these courses must be obtained ahead of time to prevent and incomplete apprenticeship--that is to say, so as to leave no room for experimentation.

Molotov cocktails, gasoline, homemade contrivances such as catapults and mortars for firing explosives, grenades made of tubes and cans, smoke bombs, mines, conventional explosives such as dynamite and potassium chloride, plastic explosives, gelatine capsules, ammunition of every kind are indispensable to the success of the urban guerrilla's mission.

The method of obtaining the necessary materials and munitions will be to by them or take them by force

in expropriation actions especially planned and carried out.

The urban guerrilla will be careful not to keep explosives and materials that can cause accidents around for very long, but will try always to use them immediately on their destined targets.

The urban guerrilla's arms and his ability to maintain them constitute his fire power. By taking advantage of modern arms and introducing innovations in his fire power and in the use of certain arms, the urban guerrilla can change many of the tactics of city warfare. An example of this was the innovation made by the urban guerrillas in Brazil when they introduced the machine gun in their attacks on banks.

When the massive use of uniform machine guns becomes possible, there will be new changes in urban guerrilla warfare tactics. The firing group that utilizes uniform weapons and corresponding ammunition, with reasonable support for their maintenance, will reach a considerable level of efficiency. The urban guerrilla increases his efficiency as he improves his firing potential.

The Shot: the Urban Guerrilla's Reason for Existence

The urban guerrilla reason for existence, the basic condition in which he acts and survives, is to shoot. The urban guerrilla must know how to shoot well because it is required by his type of combat.

In conventional warfare, combat is generally at a distance with long range arms. In unconventional warfare, in which urban guerrilla warfare is included, the combat is at close range, often very close. To prevent his own extinction, the urban guerrilla has to shoot first and he cannot err in his shot. He cannot waste his ammunition because he does not have large amounts, so he must save it. Nor can he replace his ammunition quickly, since he is part of a small group in which each guerrilla has to take care of himself. The urban guerrilla can lose no time and must be able to shoot at once.

One fundamental fact which we want to emphasize fully and whose particular importance cannot be overestimated is that the urban guerrilla must not fire continuously, using up his ammunition. It may be that the enemy is not responding to fire precisely because he is waiting until the guerrilla's ammunition is used up. At such a moment, without having time to replace his ammunition, the urban guerrilla faces a rain of enemy fire and can be taken prisoner or killed.

In spite of the value of the surprise factor which many times makes it unnecessary for the urban guerrilla to use his arms, he cannot be allowed the luxury of entering combat without knowing how to shoot. And face to face with the enemy, he must always be moving from one position to another, because to stay in one position makes him a fixed target and, as such, very vulnerable.

The urban guerrilla's life depends on shooting, on his ability to handle his arms well and to avoid being hit. When we speak of shooting, we speak of marksmanship as well. Shooting must be learned until it becomes a reflex action on the part of the urban guerrilla.

To learn how to shoot and to have good aim, the urban guerrilla must train himself systematically, utilizing every apprenticeship method, shooting at targets, even in amusement parks and at home.

Shooting and marksmanship are the urban guerrilla's water and ir. His perfection of the art of shooting makes him a special type of urban guerilla--that is, a sniper, a category of solitary combatant indispensable in isolated actions. The sniper knows how to shoot, at close range and at long range, and his arms are appropriate for either type of shooting.

The Firing Group

In order to function, the urban guerrillas must be organized in small groups. A group of no more than four or five is called *the firing group*.

A minimum of two firing groups, separated and sealed off from other firing groups, directed and coordinated by one or two persons, this is what makes a *firing team*.

Within the firing group there must be complete confidence among the comrades. The best shot at the one who best knows how to manage the machine gun is the person in charge of operations.

The firing groups plans and executes urban guerrilla actions, obtains and guards arms, studies and corrects its own tactics.

Where there are task planned by the strategic command, these tasks take preference. But there is no such thing as a firing group without its own initiative. For this reason it is essential to avoid any rigidity in the organization in order to permit the greatest possible initiative on the part of the firing group. The old-type hierarchy, the style of the traditional left doesn't exist in our organization.

This means that, except for the priority of objectives set by the strategic command, any firing group can decide to assault a bank, to kidnap or to execute an agent of the dictatorship, a figure identified with the reaction, or a North American spy, and can carry out any kind of propaganda or war of nerves against the enemy without the need to consult the general command.

No firing group can remain inactive waiting for orders from above. Its obligation is to act. Any single urban guerrilla who wants to establish a firing group and begin action can do so and thus become a part of the organization.

This method of action eliminates the need for knowing who is carrying out which actions, since there is free initiative and the only important point is to increase substantially the volume of urban guerrilla activity in order to wear out the government and to force it onto the defensive.

The firing group is the instrument of organized action. Within it, guerrilla operations and tactics are planned, launched, and carried through to success.

The general command counts on the firing groups to carry out objectives of a strategic nature, and to do so in any part of the country. For its part, it helps the firing groups with their difficulties and their needs.

The organization is an indestructible network of firing groups, and of coordinations among them, that functions, simply and practically with a general command that also participates in the attacks; an organization which exists for no purpose other than pure and simple revolutionary action.

The Logistics of the Urban Guerrilla

Conventional logistics can be expressed by the formula CCEM:

C--food (*comida*)
C--fuel (*combustivel*)
E--equipment
M--ammunition (*muniçoes*)

Conventional logistics refer to the maintenance problems for an army or a regular armed force, transported in vehicles with fixed bases and supply lines.

Urban guerrillas, on the contrary, are not an army but small armed groups, intentionally fragmented. They have no vehicles nor fixed bases. Their supply lines are precarious and insufficient, and have no established base except in the rudimentary sense of an arms factory within a house.

While the goal of conventional logistics is to supply the war needs of the guerrillas to be used to repress urban and rural rebellion, urban guerrilla logistics aim at sustaining operations and tactics which have nothing in common with a conventional war and are directed against the military dictatorship and North American domination of the country.

For the urban guerrilla, who starts from nothing and has no support at the beginning, logistics are expressed by the formula MDAME, which is:

M--mechanization
D--money (*dinheiro*)
A--arms
M--ammunition (*muniçoes*)
E--explosives

Revolutionary logistics takes mechanization as one of its bases. Nevertheless, mechanization is inseparable from the driver. The urban guerrilla driver is an important as the urban guerrilla machine gunner. Without either, the machines do not work, and as such the automobile like the machine gun becomes a dead thing. An experienced driver is not made in one day and the apprenticeship must begin early. Every good urban guerrilla must be a good driver. As to the vehicle, the urban guerrilla must expropriate what he needs.

When he already has resources, the urban guerrilla can combine the expropriation of vehicles with other methods of acquisition.

Money, arms, ammunition and explosives, and automobiles as well, must be expropriated. And the urban guerrilla must rob banks and armories and seize explosives and ammunition wherever he finds them.

None of these operations is undertaken for just one purpose. Even when the assault is for money, the

arms that the guards bear must also be taken.

Expropriation is the first step in the organization of our logistics, which itself assumes an armed and permanently mobile character.

The second step is to reinforce and extend logistics, resorting to ambushes and traps in which the enemy will be surprised and his arms, ammunition, vehicles, and other resources can be captured.

Once he has the arms, ammunition, and explosives, one of the most serious logistics problems the urban guerrilla faces at any time and in any situation is a hiding place in which to leave the material and appropriate means for transporting it and assembling it where it is needed. This has to be accomplished even when the enemy on the look out and has the roads blocked.

The knowledge that the urban guerrilla has of the terrain, and the devices he uses or is capable of using, such as guides especially prepared and recruited for this mission, are the basic elements in the solution of the eternal logistics problem the revolutionary faces.

The Technique of the Urban Guerrilla

In its most general sense, technique is the combination of methods man uses to carry out any activity. The activity of the urban guerrilla consists in waging guerrilla warfare and psychological warfare.

The urban guerrilla technique has five basic components:

a) one part is related to the specific characteristics of the situation;
b) one part is related to the requisites that match these characteristics, requisites represented by a series of initial advantages without which the urban guerrilla cannot achieve his objectives;
c) one part concerns certain and definite objectives in the actions initiated by the urban gerrilla;
d) one part is related to the types and characteristic modes of action for the urban guerrilla;
e) one part is concerned with the urban guerrilla's methods of carrying out his specific actions.

Characteristic of the Urban Guerrilla's Technique

The technique of the urban guerrilla has the following technique:

a) it is an aggressive technique, or in other words, it has an offensive character. As is well known, defensive action means death for us. Since we are inferior to the enemy in fire power and have neither his resources nor his power force, we cannot defend ourselves against an offensive or a concentrated attack by the gorillas. And that is the reason why our urban technique can never be permanent, can never defend a fixed base nor remain in any one spot waiting to repel the circle of reaction;

b) it is a technique of attack and retreat by which we preserve our forces;

c) it is a technique that aims at the development of urban guerrilla warfare, whose function will be to wear out, demoralize, and distract the enemy forces, permitting the emergence and survival of rural guerrilla warfare which is destined to play the decisive role in the revolutionary war.

The Initial Advantages of the Urban Guerrilla

The dynamics of urban guerrilla warfare lie in the urban guerrilla's violent clash with the military and police forces of the dictatorship. In this slash, the police have superiority. The urban guerrilla has inferior forces. The paradox is that the urban guerrilla, although weaker, is nevertheless the attacker.

The military and police forces, for their part, respond to the attack, by mobilizing and concentrating infinitely superior forces in the persecution and destruction of the urban guerrilla. He can only avoid defeat if he counts on the initial advantages he has and knows how to exploit them to the end to compensate for his weakness and lack of matériel.

The initial advantages are:

1) he must take the enemy by surprise;
2) he must know the terrain of the encounter better than the enemy;
3) he must have greater mobility and speed than the police and other repressive forces;
4) his information service must be better than the enemy's
5) he must be in command of the situation and demonstrate a decisiveness so great that everyone on our side is inspired and never thinks of hesitating, while on the other side the enemy is stunned and incapable of responding.

Surprise

To compensate for the general weakness and shortage of arms compared to the enemy, the urban guerrilla uses surprise. The enemy has no way to fight surprise and becomes confused or is destroyed.

When urban guerrilla warfare broke out in Brazil, experience proved that surprise was essential to the success of any urban guerrilla operation.

The technique of surprise is based on four essential requisites:

a) we know the situation of the enemy we are going to attack, usually by means of precise information and meticulous observation, while the enemy does not know he is going to be attacked and knows nothing about the attacker;

b) we know the force of the enemy that is going to be attacked and the enemy knows nothing about our force;

c) attacking by surprise, we save and conserve our forces, while the enemy is unable to do the same and is left at the mercy of events;

d) we determine the hour and the place of the attack, fix its duration, and establish its objective. The enemy remains ignorant of all this.

Knowledge of the Terrain

The urban guerrilla's best ally is the terrain and because this is so must know it like the palm of his hand.

To have the terrain as an ally means to know how to use with intelligence its unevenness, its high and low points, its turns, its irregularities, its regular and secret passages, abandoned areas, its thickets, etc., taking maximum advantage of all this for the success of armed actions, escapes, retreats, cover, and hiding places.

Its impasses and narrow spots, it gorges, its streets under repair, police control points, military zones and closed off streets, the entrances and exits of tunnels and those that the enemy can close off, viaducts to be crossed, corners controlled by the police or watched, it lights and signals, all this must be thoroughly known and studied in order to avoid fatal errors.

Our problem is to get through and to know where and how to hide, leaving the enemy bewildered in areas that he doesn't know.

Familiar with the avenues, streets, alleys, ins and outs, and corners of urban centers, its paths and shortcuts, its empty lots, its underground passages, its pipes and sewer system, the urban guerrilla safely crosses through the irregular and difficult terrain unfamiliar to the police, where they can be surprised in a fatal ambush or trapped at any moment.

Because he knows the terrain the guerrilla can go through it on foot, on bicycle, in automobile, jeep, or truck and never be trapped. Acting in small groups with only a few people, the guerrillas can reunite at an hour and place determined beforehand, following up the attack with new guerrilla operations, or even evading the police circle and disorienting the enemy with their unprecedented audacity.

It is an insoluble problem for the police in the labyrinthian terrain of the urban guerrilla, to get someone they can't see, tp repress someone they can't catch, to close in on someone they can't find.

Our experience is that the ideal urban guerrilla is one who operates in his own city and knows thoroughly it streets, its neighborhoods, its transit problems, and other peculiarities.

The guerrilla outsider, who comes to a city whose corners are unfamiliar to him, is a weak spot and if he is assigned certain operations, can endanger them. To avoid grave errors, it is necessary for him to get to know well the layout of the streets.

Mobility and Speed

To insure mobility and speed that the police cannot match, the urban guerrilla needs the following prerequisites:

a) mechanization
b) knowledge of the terrain;
c) a rupture or suspension of enemy communications and transport;
d) light arms.

By carefully carrying through operations that last only a few moments, and leaving the site in mechanized vehicles the urban guerrilla beats a rapid retreat, escaping pursuit.

The urban guerrilla must know the way in detail and, in this sense, must go through the schedule ahead of time as a training to avoid entering alleyways that have no exit, or running into traffic jams, or becoming paralyzed by the Transit Department's traffic signals.

The police pursue the urban guerrilla blindly without knowing which road he is using for his escape.

While the urban guerrilla quickly flees because he knows the terrain, the police lose the trail and give up the chase.

The urban guerrilla must launch his operations far from the logistics base of the police. An initial advantage of this method of operation is that it places us at a reasonable distance from the possibility of pursuit, which facilitates the evasion.

In addition to this necessary precaution, the urban guerrilla must be concerned with the enemy's communication system. The telephone is the primary target in preventing the enemy from having access to information by knocking out his communication system.

Even if he knows about the guerrilla operation, the enemy depends on modern transports for his logistics support, and his vehicles necessarily lose time carrying him through the heavy traffic of the large cities.

It is clear that the tangled and treacherous traffic is a disadvantage for the enemy, as it would be for us if we were not ahead of him.

If we want to have a safe margin of security and be ceratin to leave no tracks for the future, we can adopt the following methods:

a) purposely intercept the police with other vehicles or by apparently casual inconveniences and damages; but in this case the vehicles in question should not be legal nor should they have real license numbers;

b) obstruct the road with fallen trees, rocks, ditches, false traffic, signs, dead ends or detours, and other ingenious methods;

c) place homemade mines in the way of the police, use gasoline, or throw Molotov cocktails to set their vehicles on fire;

d) set off a burst of machine gun fire or arms such as the FAL aimed at the motor and the tires of the

cars engaged in pursuit.

With the arrogance typical of the police and the military fascists authorities, the enemy will come to fight us with heavy guns and equipment with elaborate maneuvers by men armed to the teeth. The urban guerrilla must respond to this with light weapons easily transported , so he can always escape with maximum speed, without ever accepting open fighting. The urban guerrilla has no mission other than to attack and retreat.

We would leave ourselves open to the most stunning defeats is we burdened ourselves with heavy arms and with the tremendous weight of the ammunition necessary to fire them, at the same time losing our precious gift of mobility.

When the enemy fights against us with calvary we are at no disadvantage as long as we are mechanized. The automobile goes faster than the horse. From within the car we also have the target of the mounted police, knocking them down with machine gun and revolver fire or with Molotov cocktails and grenades.

On the other hand, it is not so difficult for an urban guerrilla on foot to make a target of a policeman on horseback. Moreover, ropes across the streets, marbles, cork stoppers are very efficient methods of making them both fall. The great advantage of the mounted police is that he presents the urban guerrilla with two excellent targets: the horse and its rider.

Apart from being faster than the horseman, the helicopter has no better chance in pursuit. If the horse is too slow compared to the urban guerilla's automobile, the helicopter is too fast. Moving at 200 kilometers an hour it will never succeed in hitting it from above a target lost among the crowds and the street vehicles, nor can it land in public streets in order to catch someone. At the same time, when ever it tries to fly low, it will be excessively vulnerable to the fire of the urban guerrilla.

Information

The possibilities that the government has for discovering and destroying the urban guerrillas lessen as the potential of the dictatorship's enemies becomes greater and more concentrated among the popular masses.

This concentration of opponents of the dictatorship plays a very important role in providing information as to moves on the part of the police and men in government, as well as in hiding our activities. The enemy can also be throw off by false information, which is worse for him because it is a tremendous waste.

By whatever means, the sources of information at the disposal of the urban guerrilla are potentially better than those of the police. The enemy is observed by the people, but he does not know who among the people transmits information to the urban guerrilla. The military and the police are hated for the injustices they commit against the people, and this facilitates obtaining information prejudicial to the activities of government agents.

The information, which is only a small area of popular support, represents an extraordinary potential in

the hands of the urban guerrilla. The creation of an intelligence service with an organized structure is a basic need for us. The urban guerrilla has to have essential information about the plans and movements of the enemy, where they are, and how they move, the resources of the banking network, the means of communication, and the secret moves the enemy makes.

The trustworthy information passed along to the urban guerrilla represents a well-aimed blow at the dictatorship. It has no way to defend itself in the face of an important leak that jeopardizes it interests and facilitates our destructive attack.

The enemy also wants to know what steps we are taking so he can destroy us or prevent us from acting. In this sense of the danger of betrayal is present and the enemy encourages betrayal or infiltrates spies into the organization. The urban guerrilla's technique against this enemy tactic is to denounce publicly the traitors, spies, informers, and provocateurs.

Since our struggle takes place among the masses and depends on their sympathy--while the government has a bad reputation because of its brutality, corruption, and incompetence--the informers, spies, traitors, and the police come to be the enemies of the people without supporters, denounced to the urban guerrilla, and, in many cases, properly punished.

For his part the urban guerrilla must not evade the duty--once he knows who the spy or informer is--of wiping him out physically. This is the correct method, approved by the people, and it minimizes considerably the incidence of infiltration or enemy spying.

For the complete success of the battle against spies and informers, it is essential to organize a counterespionage or counterintelligence service. Nevertheless, as far as information is concerned, it cannot all be reduced to a question of knowing the enemy's moves and avoiding the infiltration of spies. Information must be broad, it must embrace everything, including the most significant matters. There is a technique of obtaining information, and the urban guerrilla must master it. Following this technique, information is obtained naturally, as a part of the life of the people.

The urban guerrilla. Living in the midst of the people and moving about among them, must be attentive to all types of conversation and human relations, learning how to disguise his interest with great skill and judgment.

In places where people work, study, live, it is easy to collect all kinds of information on payments, business, plans of all types, points of view, opinions, people's state of mind, trips, interiors of buildings, offices and rooms, operation centers, etc.

Observation, investigation, reconnaissance, and exploration of the terrain are also excellent sources of information. The urban guerrilla never goes anywhere absent mindedly and without revolutionary precaution, always on the lookout lest something occur. Eyes and ears open, senses alert, his memory engraved with everything necessary, now or in the future, to the uninterrupted activity of the fighter.

Careful reading of the press with particular attention to the organs of mass communication, the investigation of accumulated data, the transmission of news and everything of note, a persistence being informed and in informing others, all this makes up the intricate and immensely complicated question of information which gives the urban guerrilla a decisive advantage.

Decision

It is not enough for the urban guerrilla to have in his favor surprise, speed, knowledge of the terrain, and information. He must also demonstrate his command of any situation and a capacity for decision without which all other advantages will prove useless.

It is impossible to carry out any action, however well planned, if the urban guerrilla turns out to be indecisive, uncertain, irresolute.

Even an action successively begun can end in defeat if the command of the situation and the capacity for decision falter in the middle of the actual execution of the plan. When this command of the situation and a capacity for decision are absent, the void is filled with vacillation and terror. The enemy takes advantage of this failure and is able to liquidate us.

The secret for the success of any operation, simple or complicated, easy or difficult, is to rely on determined men. Strictly speaking, there are no easy operations. All must be carried out with the same care exercised in the case of the most difficult, beginning with the choice of the human element, which means relying on leadership and capacity for decision in every test.

One can see ahead of time whether an action will be successful or not by the way its participants act during the preparatory period. Those who are behind, who fail to make designated contacts, are easily confused, forget things, fail to complete+ the basic elements of the work, possibly are indecisive men and can be a danger. It is better not to include them.

Decision means to put into practice the plan that has been devised with determination, with audacity, and with an absolute firmness. It takes only one person who vacillates to lose it all.

Objectives of the Urban Guerrilla's Actions

With his technique developed and established, the urban guerrilla bases himself on models of action leading to attack and, in Brazil, with the following objectives:

a) to threaten the triangle in which the Brazilian state system and North American domination are maintained in Brazil, a triangle whose points are Rio, Sao Paulo, and Belo Horizonte and whose base is the axle Rio-Sao Paulo, where the giant industrial-financial-economic-political-cultural-military-police complex that holds the entire decisive power of the country is located;

b) to weaken the local guards or the security system of the dictatorship, given the fact that we are attacking and the gorillas are defending, which mens catching the government in a defensive position with its troops immobilized in defense of the entire complex of national maintenance, with its ever-present fears of an attack on a strategic nerve centers, and without ever knowing where, how, and when the attack will come;

c) to attack on every side with many different armed groups, few in number, each self-contained and

operating separately, to disperse the government forces in their pursuit of a thoroughly fragmented organization instead of offering the dictatorship the opportunity to concentrate its forces of repression on the destruction of one tightly organized system operating throughout the country;

d) to give proof of its combativeness, decision, firmness, determination, and persistence in the attack on the military dictatorship in order to permit all malcontents to follow our example and fight with urban guerrilla tactics. Meanwhile, the government, with all its problems, incapable of halting guerrilla operations in the city, will lose time and suffer endless attrition and will finally be forced to pull back its repressive troops in order to mount guard over the banks, industries, armories, military barracks, prisons, public offices, radio and television stations, North American firms, gas storage tanks, oil refineries, ships, airplanes, ports, airports, hospitals, health centers, blood banks, stores, garages, embassies, residences of outstanding members of the regime, such as ministers and generals, police stations, and official organizations, etc.;

e) to increase urban guerrilla disturbances gradually in an endless ascendancy of unforeseen actions such that the government troops cannot leave the urban area to pursue the guerrillas in the interior without running the risk of abandoning the cities and permitting rebellion to increase on the coasts as well as in the interior of the country;

f) to oblige the army and the police, with the commanders and their assistants, to change the relative comfort and tranquility of their barracks and their usual rest, for a state of alarm and growing tension in the expectation of attack or in search of tracks that vanish without a trace;

g) to avoid open battle and decisive combat with the government, limiting the struggle to brief and rapid attacks with lightening results;

h) to assure for the urban guerrilla a maximum freedom of maneuvers and action without ever relinquishing the use of armed violence, remaining firmly oriented toward helping the beginning of rural guerrilla warfare and supporting the construction of the revolutionary army for national liberation.

On the Types and Nature of Action Models for the Urban Guerrilla

In order to achieve the objects previously enumerated, the urban guerrilla is obliged in his technique, to follow an action whose nature is as different and as diversified as possible. The urban guerrilla does not arbitrarily choose this or that action model. Some actions are simple, others are complicated. The urban guerrilla without experience must be incorporated gradually into actions and operations that run from the simple to the complex. He begins with small missions and tasks until he becomes a completely experienced urban guerrilla.

Before any action, the urban guerrilla must think of the methods and the personnel at his disposal to carry out the action. Operations and actions that demand the urban guerrilla's technical preparation cannot be carried out by someone who lacks that technical skill. With these cautions, the action models which the urban guerrilla can carry out are the following:

a) assaults;
b) raids and penetrations;

c) occupations;
d) ambush;
e) street tactics;
f) strikes and work interruptions;
g) desertions, diversions, seizures, expropriation of arms, ammunition, explosives;
h) liberation of prisoners;
i) executions;
j) kidnappings;
k) sabotage;
l) terrorism;
m) armed propaganda;
n) war of nerves.

Assaults

Assault is the armed attack which we make to expropriate funds, liberate prisoners, capture explosives, machine guns, and other types arms and ammunition.

Assaults can take place in broad daylight or at night.

Daytime assaults are made when the objective cannot be achieved at any other hour, as for example, the transport of money by the banks, which is not done at night.

Night assault is usually the most advantageous to the urban guerrilla. The ideal is for all assaults to take place at night when conditions for a surprise attack are most favorable and the darkness facilitates flight and hides the identity of the participants. The urban guerrilla must prepare himself, nevertheless, to act under all conditions, daytime as well as nighttime.

The vulnerable targets for assaults are the following:

a) credit establishments
b) commercial and industrial enterprises, including the production of arms and explosives;
c) military establishments
d) commissaries and police stations;
e) jails;
f) government property;
g) mass communication media;
h) North American firms and properties;
i) government vehicles, including military and police vehicles, trucks, armored vehicles, money carriers, trains, ships, and planes.

The assaults on establishments are the same in nature because in every case the property and buildings represent a fixed target.

Assaults on buildings are conceived as guerrilla operations, varied according to whether they are against banks, a commercial enterprise, industries, military camps, commissaries, prisons, radio stations,

warehouses for imperialist firms, etc.

The assaults on vehicles-money-carriers, armored cars, trains, ships, airplanes--are of another nature since they are moving targets. The nature of the operations varies according to the situation and the possibility--that is whether the target is stationary or moving.

Armored cars including military cars, are not immune to mines. Obstructed roads, traps, ruses, interception of other vehicles, Molotov cocktails, shooting with heavy arms, are efficient methods of assaulting vehicles.

Heavy vehicles, grounded planes, anchored ships can be seized and their crew and guards

overcome. Airplanes in flight can be diverted from their course by guerrilla action or by one person.

Ships and trains in movement can be assaulted or taken by guerrilla operations in order to capture the arms and munitions or to prevent troop deployment.

The Bank Assault as a Popular Model

The most popular assault model is the bank assault. In Brazil, the urban guerrilla has begun a type of organized assault on the banks and as a guerrilla operation. Today this type of assault is widely used and has served as a sort of preliminary examination for the urban guerrilla in his apprenticeship for the techniques of revolutionary warfare.

Important innovations in this technique of assaulting banks have developed, guaranteeing flight, the withdrawal of money, and the anonymity of those involved. Among these innovations we cite shooting the tires of cars to prevent pursuit; locking people in the bank bathroom, making them sit on the floor; immobilizing the bank guards and removing their arms, forcing someone to open the coffer or the strong box; using disguises.

Attempts to install bank alarms, to use guards or electronic detection devices of U.S. origin, prove fruitless when the assault is political and is carried out according to urban guerrilla b warfare technique. This technique tries to utilize new resources to meet to meet the enemies tactical changes, has access to a fire power that is growing every day, becomes increasingly astute and audacious, and uses a large number of revolutionaries every time; all to guarantee the success of operations planned down to the last detail.

The bank assault is a typical expropriation. But, as is true in any kind of armed expropriatory action, the revolutionary is handicapped by a two-fold competition:

a) competition from the outlaw;

b) competition from the right-wing counterrevolutionary.

This competition produces confusion, which is reflected in the people's uncertainty. It is up to the urban guerrilla to prevent this from happening, and to accomplish this he must use two methods:

a) he must avoid the outlaw's technique, which is one of unnecessary violence and appropriation of good and possessions belonging to the people;

b) he must use the assault for propaganda purposes, at the very moment it is taking place, and later distribute material, leaflets, every possible means of explaining the objectives and the principles of the urban guerrilla as expropriator of the government, the ruling classes, and imperialism.

Raids and Penetration

Raids and penetrations are quick attacks on establishments located in neighborhoods or even in the center of the city, such as small military units, commissaries, hospitals, to cause trouble, seize arms, punish and terrorize the enemy, take reprisal, or rescue wounded prisoners, or those hospitalized under police vigilance.

Raids and penetrations are also made on garages and depots to destroy vehicles and damage installations, especially if they are North American firms and property.

When they take place on certain stretches of the highway or in certain distant neighborhoods, the raids can serve to force the enemy to move great numbers of troops, a totally useless effort since he will find nobody there to fight.

When they are carried out in certain houses, offices, archives, or public offices, their purpose is to capture, or search for secret papers and documents with which to denounce involvements, comprises, and the corruption of men in the government, their dirty deals and criminal transactions with the North Americans.

Raids and penetrations are most effective if they are carried out at night.

Occupations

Occupations are the type of attack carried out when the urban guerrilla stations himself in specific establishments and locations for a temporary resistance against the enemy or for some propaganda purpose.

The occupation of factories and schools during strikes or at other times is a method of protest or of distracting the enemy's attention.

The occupation of radio stations is for propaganda purposes.

Occupation is a highly effective model for action but, in order to prevent losses and material damage to our ranks, it is always a good idea to count on the possibility of withdrawal. It must always be meticulously planned and carried out at the opportune moment.

Occupation always has a time limit and the faster it is completed the better.

Ambush

Ambushes are attacks typified by surprise when the enemy is trapped across a road or when he makes a police net surrounding a house or an estate. A false message can bring the enemy to the spot where he falls into the trap.

The principle object of the ambush tactic is to capture enemy arms and punish him with death.

Ambushes to halt passenger trains are for propaganda purposes and, when they are troop trains, the object is to annihilate the enemy and seize his arms.

The urban guerrilla sniper is the kind of fighter especially suited for ambush because he can hide easily in the irregularities of the terrain, on the roof and tops of buildings and apartments under construction. From windows and dark places, he can take careful aim at his chosen target.

Ambush has devastating effects on the enemy, leaving him unnerved, insecure, and fearful.

Street Tactics

Street tactics are used to fight the enemy in the streets, utilizing the participation of the masses against him.

In 1968 the Brazilian students used excellent street tactics against police troops, such as marching down streets against traffic, utilizing slings and marbles as arms against the mounted police.

Other street tactics consist in constructing barricades; pulling up paving blocks and hurling them at the police; throwing bottles, bricks, paperweights, and other projectiles from the tops of apartment and office buildings against the police; using buildings under construction for flight, hiding, and for supporting surprise attacks.

It is equally necessary to know how to respond to enemy tactics. When the police troops come protected with helmets to defend themselves against flying objects, we have to divide ourselves into two teams: one to attack the enemy from the front, the other to attack him in the rear, withdrawing one as the other goes into action to prevent the first from becoming a target for projectiles hurled by the second.

By the same token it is important to know how to respond to the police net. When the police designate certain of their men to go into the masses to arrest a demonstrator, a larger group of urban guerrillas must surround the police group, disarming and beating them and at the same time letting the prisoner escape. This urban guerrilla operation is called the *net within the net*.

When the police net is formed at a school building, a factory, a place where the masses assemble, or some other point, the urban guerrilla must not give up or allow himself to be taken by surprise. To make his net work the enemy is to transport the police vehicles and special cars to occupy strategic points in the streets in order to invade the building or chosen locale. The urban guerrilla, for his part, must never clear a building or an area and meet in it without first knowing its exits , the way to break the circle, the strategic points that the police might occupy, and the roads that inevitably lead into the net, and he must hold other strategic points from which to strike at the enemy.

The roads followed by the police vehicles must be mined at key points along the way and at forced stopping points. When the mines explode, the vehicles will fly into the air. The police will be caught in the trap and will suffer losses or will be victims of ambush. The net must be broken by escape routes unknown to the police. The rigorous planning of the retreat is the best way of frustrating any encircling effort on the part of the enemy.

When there is no possibility of a flight plan, the urban guerrilla must not hold meetings, assemblies, or do anything else since to do so will prevent him from breaking through the net the enemy will surely try to throw him around.

Street tactics have revealed a new type of urban guerrilla, the urban guerrilla who participates in mass demonstrations. This is the type we designate as the urban guerrilla demonstrator, who joins the ranks and participates in popular marches with specific and definite aims.

These aims consist in hurling stones and projectiles of every type, using gasoline to start fires, using the police as a target for their fire arms, capturing police arms, kidnapping agents of the enemy and provocateurs, shooting with careful aim at the henchmen torturers and the police chiefs who come in special cars with false plates in order not to attract attention.

The urban guerrilla demonstrator shows in the mass demonstration the flight route if that is necessary. He plants mines, throws Molotov cocktails, prepares ambushes and explosions.

The urban guerrilla demonstrator must also initiate the *net within the net*, going through government vehicles, official cars, and police vehicles before turning them over or setting them on fire, to see if any of them have money and arms.

Snipers are very good for mass demonstrations and, along with the urban guerilla demonstrators, can play a valuable role.

Hidden at strategic points, the snipers have complete success, using shotguns, machine guns, etc. whose fire and ricocheting easily cause losses among the enemy.

Strikes and Work Interruptions

The strike is a model of action employed by the urban guerrilla in work centers and schools to damage the enemy by stopping work study activities. Because it is one of the weapons most feared by the exploiters and oppressors, the enemy uses tremendous fighting power and incredible violence against it. The strikers are taken to prison, suffer beatings, and many of them wind up assassinated.

The urban guerrilla must prepare the strike in such a way as to leave no tracks or clues that identify the leaders of the action. A strike is successful when it is organized through the action of a small group, if it is carefully prepared in secret and by the most clandestine methods.

Arms, ammunition. Molotovs, homemade weapons of destruction and attack, all this must be supplied beforehand in order to meet the enemy. So that it can do the greatest possible damage, it is a good idea to study and put into a sabotage plan.

Work and study interruptions, although they are of brief duration, cause severe damage to the enemy. It is enough for them to crop up at different points and in different sections of the same area, disrupting daily life, occurring endlessly one after the other, in authentic guerrilla fashion.

In strikes or simple work interruptions, the urban guerrilla has recourse to occupation or penetration of the locale or can simply make a raid. In that case his objective is to take hostages, to capture prisoners, or to kidnap enemy agents and propose an exchange for the arrested strikers.

In certain cases, strikes and brief work interruptions can offer an excellent opportunity for preparing ambushes or traps whose aim is the physical liquidation of the cruel, bloody police.

The basic fact is that the enemy suffers losses and material and moral damage, and is weakened by the action.

Desertions, Diversions, Seizures, Expropriations of Arms, Ammunition, Explosives

Desertion and the diversion of arms are actions effected in military camps, ships, military hospitals, etc. The urban guerrilla soldier, chief, sergeant, subofficial, and official must desert at the opportune moment with modern arms and ammunition to hand them over for the use of the Brazilian revolution.

One of the opportune moments is when the military urban guerrilla is called upon to pursue and fight his guerrilla comrades outside the military quarters. Instead of following the orders of the gorillas, the military urban guerrilla must join the revolutionaries by handing over the arms and ammunition he carries, of the military plane he pilots.

The advantage of this method is that the revolutionaries receive arms and ammunition from the army, the navy, and the air force, the military police, the civilian guard, or the firemen without any great work, since it reaches their hands by government transport.

Other opportunities may occur in the barracks, and the military urban guerrilla must always be alert to this. In case of carelessness on the part of the commanders or in other favorable conditions, such as bureaucratic attitudes and behavior or relaxation of discipline on the part of sub-lieutenants and other internal personnel, the military urban guerrilla must no longer wait but must try to advise the organizations and desert alone or accompanied, but with as large a supply of arms as possible.

With information from and participation of the military urban guerrilla, raids on barracks and other military establishments for the purpose of capturing arms can be organized.

When there is no possibility of deserting and taking arms and ammunition, the military urban guerrilla must engage in sabotage, starting explosions and fires in munitions and gunpowder.

This technique of deserting with arms and ammunition, or raiding and sabotaging the military centers, is the best way of wearing out and demoralizing the gorillas and of leaving them confused.

The urban guerrilla's purpose in disarming an individual enemy is to capture his arms. These arms are usually in the hands of the sentinels or others whose task is guard duty or repression.

The capture of arms may be accompanied by violent means or by astuteness and by tricks or traps. When the enemy is disarmed, he must be searched for arms other than those already taken from him. If we are careless, he can use the arms that were not seized to shoot the urban guerrilla.

The seizure of arms is an efficient method of acquiring machine guns, the urban guerrilla's most important arms.

When we carry out small operations or actions to seize arms and ammunition, the material captured my be for personal use or for armaments and supplies for the firing groups.

The necessity to provide firing power for the urban guerrilla is so great that in order to take off from zero point we often have to purchase one weapon, divert or capture a single arm. The basic point is to begin, and to begin with a great spirit of decisiveness and of boldness. The possession of a single arm multiplies our forces.

In a bank assault, we must be careful to seize the arm or arms of the bank guard. The remainder of the arms we find with the treasurer, the bank teller, or the manager must also be seized ahead of time.

The other method we can use to capture arms is the preparation of ambushes against the police and the cars they use to move around in.

Quite often we succeed in capturing arms in the police commissaries as a result of raids from outside.

The expropriation of arms, ammunition, and explosives is the urban guerrilla's goal in assaulting commercial houses, industries, and quarries.

Liberation of Prisoners

The liberation of prisoners is an armed operation designed to free the jailed urban guerrilla. In daily struggle against the enemy, the urban guerrilla is subject to arrest and can be sentenced to unlimited years in jail. This does not mean that the revolutionary battle stops here. For the guerrilla, his experience is deepened by prison and continues even in the dungeons where he is held.

The imprisoned urban guerrilla views jail as a terrain he must dominate and understand in order to free himself by a guerrilla operation. There is no prison, either on an island, in a city penitentiary, or on a farm, that is impregnable to slyness, the cleverness, and the firing potential of the revolutionaries.

The urban guerrilla who is free views the penal establishments of the enemy as the inevitable site of guerrilla action designed to liberate his ideological brothers from prison.

It is this combination of *the urban guerrilla in freedom and the urban guerrilla in jail* that results in the armed operations we refer to as the liberation of prisoners.

The guerrilla operations that can be used in liberating prisoners are the following:

a) riots in penal establishments, in correctional colonies and islands or on transport or prison ships;
b) assaults on urban or rural penitentiaries, houses of detention, commissaries, prisoner depots, or any other permanent, occasional, or temporary place where prisoners are held;
c) assaults on prisoner transport trains and cars;
d) raids and penetrations of prisons;
e) ambushing of guards who are moving prisoners.

Execution

Execution is the killing of a North American spy, of an of the dictatorship, of a police torturer, of a fascist personality in the government involved in crimes and persecutions against patriots, of a stool pigeon, informer, police agent, or police provocateur.

Those who go to the police of their own free will to make denunciations and accusations, who supply clues and information and finger people, must also be executed when they are caught by the urban guerrilla.

Execution is a secret action in which the least possible number of urban guerrillas are involved. In many cases, the execution can be carried out by one sniper, patiently, alone and unknown, and operating in absolute secrecy in cold blood.

Kidnaping

Kidnaping is capturing and holding in a secret spot a police agent, a North American spy, a political personality, or a notorious and dangerous enemy of the revolutionary movement.

Kidnaping is used to exchange or liberate imprisoned revolutionary comrades, or to force suspension of torture in the jail cells of the military dictatorship.

The kidnaping of personalities who are known artists, sports figures, or are outstanding in some other field, but who have evidenced no political interest, can be a useful form of propaganda for the revolutionary and patriotic principles of the urban guerrilla provided it occurs under special circumstances, and the kidnaping is handled so that the public sympathizes with it and accepts it.

The kidnaping of North American residents or visitors in Brazil constitutes a form of protest against the penetration and domination of United States imperialism in our country.

Sabotage

Sabotage is a highly destructive type of attack using very few persons and sometimes requiring only one to accomplish the desired result. When the urban guerrilla uses sabotage the first phase is isolated sabotage. Then comes the phase of dispersed and generalized sabotage, carried out by the people.

Well-executed sabotage demands study, planning, and careful execution. A characteristic form of sabotage is explosion using dynamite, fire, and the placing of mines.

A little sand, a trickle of any kind of combustible, a poor lubrication, a screw removed, a short circuit, pieces of wood or of iron, can cause irreparable damage.

The objective of sabotage is to hurt, to damage, to make useless, and to destroy vital enemy points such as the following:

a) the economy;
b) agricultural or industrial production:
c) transport and communication systems;
d) the military and police systems and their establishments and deposits;
e) the repressive military-police system;
f) the firms and properties of North Americans in the country.

The urban guerrilla should endanger the economy of the country, particularly its economic and financial aspects, such as its domestic and foreign commercial network., its exchange and banking systems, its tax collection systems, and others.

Public offices, centers of government services, government warehouses, are easy targets for sabotage.

Nor will it be easy to prevent the sabotage of agricultural and industrial production by the urban guerrilla, with his thorough knowledge of the local situation.

Industrial workers acting as urban guerrillas are excellent industrial saboteurs since they, better than anyone, understand the industry, the factory, the machine, or the part most likely to destroy an entire operation, doing far more damage than a poorly informed layman could do.

With respect to the enemy's transport and communications system, beginning with railway traffic, it is necessary to attack them systematically with sabotage arms.

The caution is against causing death and fatal injury to passengers, especially regular commuters on suburban and long-distance trains.

Attacks on freight trains, rolling or stationary stock, stoppage of military transport and communication systems, these are the major sabotage objectives in this area.

Sleepers can be damaged and pulled up, as can rails. A tunnel blocked by a barrier after an explosion, an obstruction by a derailed car, cause tremendous harm.

The derailment of a cargo train carrying fuel is of major damage to the enemy. So is dynamiting railway bridges. In a system where the weight and the size of the rolling equipment is enormous, it takes months for workers to repair or rebuild the destruction and the damage.

As for highways, they can be obstructed by trees, stationary vehicles, ditches, dislocation of barriers by dynamite, and bridges blown up by explosion.

Ships can be damaged at anchor in seaports and river ports or in the shipyards. Airplanes can be destroyed or sabotaged on the ground.

Telephonic and telegraphic lines can be systematically damaged, their towers blown up, and their lines made useless.

Transport and communications must be sabotaged at once because the revolutionary war has begun in Brazil and it is essential to impede the enemy's movement of troops and munitions.

Oil lines, fuel plants, depots for bombs and ammunition, powder magazines and arsenals, military camps, commissaries must be targets par excellence in sabotage operations, while vehicles, army trucks, and other military and police cars must be destroyed wherever they are found.

The military and police repression centers and their specific and specialized organs, must also claim the attention of the urban guerrilla saboteur.

North American firms and properties in the country, for their part, must become such frequent targets of sabotage that the volume of actions directed against them surpasses the total of all other actions against vital enemy points.

Terrorism

Terrorism is an action, usually involving the placement of a bomb or fire explosion of great destructive power, which is capable of effecting irreparable loss against the enemy.

Terrorism requires that the urban guerrilla should have an adequate theoretical and practical knowledge of how to make explosives.

The terroristic act, apart from the apparent facility with which it can be carried out, is no different from other urban guerrilla acts and actions whose success depends on the planning and determination of the revolutionary organization. It is an action that the urban guerrilla must execute with the greatest cold bloodedness, calmness, and decision.

Although terrorism generally involves an explosion, there are cases in which it may also be carried out by execution and the systematic burning of installations, properties, and North American depots, plantations, etc. It is essential to point out the importance of fires and the construction of incendiary

bombs such as gasoline bombs in the technique of revolutionary terrorism. Another thing is the importance of the material the urban guerrilla can persuade the people to expropriate in moments of hunger and scarcity resulting from the greed of the big commercial interests.

Terrorism is an arm the revolution can never relinquish.

Armed Propaganda

The coordination of urban guerrilla actions, including each armed action is the principal way of making armed propaganda.

These actions carried out with specific and determined objectives, inevitably become propaganda material for the mass communications system.

Bank assaults, ambushes, desertions and diverting of arms, the rescue of prisoners, executions, kidnappings, sabotage, terrorism, and the war of nerves, are all cases in point.

Airplanes diverted in flight by revolutionary action, moving ships and trains assaulted and seized by guerrillas, can also be solely for propaganda effects. But the urban guerrilla must never fail to install a clandestine press and must be able to turn out mimeographed copies using alcohol or electric plates and other duplicating apparatus, expropriating what he cannot buy in order to produce small clandestine newspapers, pamphlets, flyers, and stamps for propaganda and agitation against the dictatorship.

The urban guerrilla engaged in clandestine printing facilities enormously the incorporation of large numbers of people into the revolutionary struggle, by opening a permanent work front for those willing to carry on revolutionary propaganda, even when to do so means acting alone and risking their lives as revolutionaries.

With the existence of clandestine propaganda and agitative material, the inventive spirit of the urban guerrilla expands and creates catapults, artifacts, mortars, and other instruments with which to distribute the anti-government pamphlets at a distance.

Tape recordings, the occupation of radio stations, and the use of loud speakers, drawings on walls and in other inaccessible places are other forms of propaganda.

In using them, the urban guerrilla should give them the character of armed operations.

A consistent propaganda by letters sent to specific addresses, explaining the meaning of the urban guerrillas' armed actions, produces considerable results and is one method of influencing certain segments of the population.

Even this influence exercised in the heart of the people by every possible propaganda device revolving around the activity of the urban guerrilla does not indicate that our forces have everyone's support.

It is enough to win the support of a part of the people and this can be done by popularizing the following slogan: "Let he who does not wish to do anything for the revolutionaries, do nothing against them."

The War of Nerves

The war of nerves or psychological war is an aggressive technique, based on the direct or indirect use of mass means of communication and news transmitted orally in order to demoralize the government.

In psychological warfare the government is always at a dis advantage since it imposes censorship on the mass media and winds up in a defensive position by not allowing anything against it to filter through.

At this point it becomes desperate, is involved in greater contradictions and loss of prestige, and losses time and energy in an exhausting effort at control which is subject to being broken at any moment.

The object of the war of nerves is to misinform, spreading lies among the authorities, in which everyone can participate, thus creating an air of nervousness, discredit, insecurity, uncertainty, and concern on the part of the government.

The best methods used by the urban guerrilla in the war of nerves are the following:

a) using the telephone and the mail to announce false clues to the police and the government, including information on the plating of bombs and any other act of terrorism in public offices and other places, kidnaping and assassination plans, etc., to oblige the authorities to wear themselves out, following up the information fed them;

b) letting false plans fall into the hands of the police to divert their attention;

c) planting rumors to make the government uneasy;

d) exploiting by every means possible the corruption, the errors, and failures of the government and its representatives, forcing them into demoralizing explanations and justifications in the very mass communication media they maintain under censorship;

e) presenting denunciations to foreign embassies, the United Nations, the papal nunciature, and the international judicial commissions defending human rights or freedom of the press, exposing each concrete violation and use of violence by the military dictatorship and making it known that the revolutionary war will continue its course with serious danger for the enemies of the people.

How to Carry Out the Action

The urban guerrilla who correctly carries through his apprenticeship and training must give the greatest importance to his method of carrying out action, for in this he cannot commit the slightest error.

Any carelessness in the assimilation of the method and its use invites certain disaster, as experience teaches everyday.

The outlaws commit errors frequently because of their methods, and this is one of the reasons why the urban guerrilla must be so insistently preoccupied with the following revolutionary technique and not the technique of the bandits.

And not only for that reason. There is no urban guerrilla worthy of the name who ignores the revolutionary method of action and fails to practice it rigorously in the planning and execution of his activity.

The giant is known by his toe. The same can be said of the urban guerrilla who is known from afar for his correct methods and his absolute fidelity to principles.

The revolutionary method of carrying out action is strongly and forcefully based on the knowledge and use of the following elements:

a) investigation of information;
b) observation or *paquera*;
c) reconnaissance or exploration of the terrain
d) study and timing of routes;
e) mapping;
f) mechanization;
g) selection of personnel and relief;
h) selection of firing capacity:
i) study and practice in completion
j) completion;
k) cover;
l) retreat;
m) dispersal;
n) liberation or transfer of prisoners;
o) elimination of clues;
p) rescue of wounded.

Some Observations on the Method

When there is no information, the point of departure for the planning of the action must be investigation, observation, or *paquera*. This method also has good results.

In any event, including when there is information, it is essential to take observations or *paquera*, to see that the information is not at odds with observation or vice versa.

Reconnaissance or exploration of the terrain, study and timing of routes are so important that to omit them is to make a stab in the dark.

Mechanization, in general, is an underestimated factor in the method of conducting the action. Frequently mechanization is left to the end, to the eve of the action, before anything is done about it.

This is an error. Mechanization must be considered seriously, must be undertaken with considerable foresight and according to careful planning, also based on information, observation or *paquera*, and must be carried out with rigorous care and precision. The care, conservation, maintenance, and camouflaging of the vehicles expropriated are very important details of mechanization.

When transport fails, the principle action fails with serious moral and material consequences for the urban guerrilla activity.

The selection of personnel requires great care to avoid the inclusion of indecisive or vacillating personnel with the danger of contaminating the other participants , a difficulty that must be avoided.

The withdrawal is equally or more important than the operation itself, to the point that it must be rigorously planned, including the possibility of failure.

One must avoid rescue or transfer of prisoners with children present, or anything to attract the attention of people in casual transit through the area. The best thing is to make the rescue as natural as possible, always winding through, or using different routes or narrow streets that can scarcely permit passage on foot , to avoid an encounter of two cars. The elimination of tracks is obligatory and demands the greatest caution in hiding fingerprints and any other sign that could give the enemy information. Lack of care in the elimination of tracks and clues is a factor that increases nervousness in our ranks and which the enemy often exploits.

Rescue of the Wounded

The problem of the wounded in urban guerrilla warfare merits special attention. During guerrilla operations in the urban area it may happen that some comrade is accidentally wounded or shot by the police. When a guerrilla in the firing group has a knowledge of first aid he can do something for the wounded comrade on the spot. In no circumstances can the wounded urban guerrilla be abandoned at the site of the battle or left to the enemy's hands.

One of the precautions we must take is to set up nursing courses for men and women, courses in which the urban guerrilla can matriculate and learn the elementary techniques of first aid.

The urban guerrilla doctor, student of medicine, nurse, pharmacologist, or simply the person trained in first aid, is a necessity in modern revolutionary struggle.

A small manual of first aid for the urban guerrilla, printed on mimeographed sheets, can also be undertaken by anyone who has enough knowledge.

In planning and completing an armed action, the urban guerrilla cannot forget the organization of medical logistics. This will be accomplished by means of a mobile or motorized clinic. You can also set up a mobile first aid station. Another solution is to utilize the skills of a nursing comrade who waits with his bag of equipment in a designated house to which the wounded are brought.

The ideal would be to have our own well equipped clinic, but this is very costly unless we use expropriated materials.

When all else fails, it is often necessary to resort to legal clinics, using armed force if necessary to demand that the doctors attend to our wounded.

In the eventuality that we fall back on blood banks to buy blood or whole plasma, we must not use legal

addresses and certainly not addresses where the wounded can really be found, since they are under our care and protection. Nor should we supply addresses of those involved in the organization's clandestine work to the hospitals and health centers where we take them. Such concern are indispensable to cover any track or clue.

The houses in which the wounded stay cannot be known to anybody with the unique and exclusive exception of the small group of comrades responsible for their treatment and transport.

Sheets, bloody clothing, medicine, and any other indication of treatment of the comrades wounded in combat with the police, must be completely eliminated from any place they visit to receive medical treatment.

Guerrilla Security

The urban guerrilla lives in constant danger of the possibility of being discovered or denounced. The chief security problem is to make certain that we are well hidden and well guarded, and that there are secure methods to keep the police from locating us or our whereabouts.

The worst enemy of the urban guerrilla and the major danger we run is infiltration into our organization by a spy or an informer.

The spy trapped within the organization will be punished with death. The same goes for those who desert and inform the police.

A good security is the certainty that the enemy has no spies and agents infiltrated in our midst and can receive no information about us even by indirect or distant means. The fundamental way to insure this is to be cautious and strict in recruiting.

Nor is it permissible for everyone to know everyone and everything else. Each person should know only what related to his work. This rule is a fundamental point in the abc's of urban guerrilla security.

The battle that we are waging against the enemy is arduous and difficult because it is a class struggle. Every class struggle is a battle of life or death when the classes are antagonistic.

The enemy wants to annihilate us and fights relentlessly to find us and destroy us, so that our great weapon consists in hiding from him and attacking him by surprise.

The danger to the urban guerrilla is that he may reveal himself through imprudence or allow himself to be discovered through lack of class vigilance. It is inadmissible for the urban guerrilla to give out his own or any other clandestine address to the enemy or to talk too much. Annotations in the margins of newspapers, lost documents, calling cards, letters or notes, all these are clues that the police never underestimate.

Address and telephone books must be destroyed and one must not write or hold papers; it is necessary to avoid keeping archives of legal or illegal names, biographical information, maps, and plans. The points of contact should not be written down but simply committed to memory.

The urban guerrilla who violated these rules must be warned by the first one who motes his infraction and, if he repeats it, we must avoid working with him.

The need of the urban guerrilla to move about constantly and the relative proximity of the police, given the circumstances of the strategic police net which surrounds the city, forces him to adopt variable security methods depending on the enemy's movements.

For this reason it is necessary to maintain a service of daily news about what the enemy appears to be doing, where his police net is operating and what gorges and points of strangulation are being watched. The daily reading of the police news in the newspapers is a great fountain of information in these cases.

The most important lesson for guerrilla security is never, under any circumstances, to permit the slightest sign of laxity in the maintenance of security measures and regulations with in the organization.

Guerrilla security must be maintained also and principally in cases of arrest. The arrested guerrilla can reveal nothing to the police the will jeopardize the organization. He can say nothing that may lead, as a consequence, to the arrest of other comrades, the discovery of addresses and hiding places, the loss of arms and ammunition.

The Seven Sins of the Urban Guerrilla

Even when the urban guerrilla applies his revolutionary technique with precision and rigorously abides by security rules, he can still be vulnerable to errors. There is no perfect urban guerrilla. The most he can do is to make every effort diminish the margin of error since he cannot be perfect.

One of the methods we should use to diminish the margin of error is to know thoroughly the seven sins of the urban guerrilla and try to fight them.

The first sin of the urban guerrilla is inexperience. The urban guerrilla, blinded by this sin, thinks the enemy is stupid, underestimates his intelligence, believes everything is easy and, as a result, leaves clues that can lead to his disaster.

Because of his inexperience, the urban guerrilla can also overestimate the forces of the enemy, believing them to be stronger than they really are. Allowing himself to be fooled by this presumption, the urban guerrilla becomes intimidated, and remains insecure and indecisive, paralyzed and lacking audacity.

The second sin of the urban guerrilla is to boast about the actions he has completed and broadcast them to the four winds.

The third sin of the urban guerrilla is vanity. The urban guerrilla who suffers from this sin tries to solve the problems of the revolution by actions erupting in the city, but without bothering about the beginnings and the survival of the guerrilla in rural areas. Blinded by success, he winds up organizing an action that he considers decisive and that puts into play all the forces and resources of the organization. Since the city is the area of the strategic circle which we cannot avoid or break while rural guerrilla warfare has not yet erupted and is not at the point of triumph, we always run the fatal error of permitting the enemy to attack us with decisive blows.

The fourth sin of the urban guerrilla is to exaggerate his strength and to undertake projects for which he lacks forces and, as yet, does not have the required infrastructure.

The fifth sin of the urban guerrilla is precipitous action. The urban guerrilla who commits this sin loses patience, suffers an attack of nerves, does not wait for anything, and impetuously throws himself into action, suffering untold reverses.

The sixth sin of the urban guerrilla is to attack the enemy when he is most angry.

The seventh sin of the urban guerrilla is to fail to plan things and to act out of improvisation.

Popular Support

One of the permanent concerns of the urban guerrilla is his identification with popular causes to win public support.

Where government actions become inept and corrupt, the urban guerrilla should not hesitate to step in to show that he opposes the government and to gain mass sympathy. The present government, for example, imposes heavy financial burdens and excessively high taxes on the people. It is up to the urban guerrilla to attack the dictatorship's tax collection system and to obstruct its financial activity, throwing all the weight of violent revolutionary action against it.

The urban guerrilla fights not only to upset the tax and collection system: the arm of revolutionary violence must also be directed against those government organs that raise prices and those who direct them, as well as against the wealthiest of the national and foreign profiteers and the important property owners; in short against all those who accumulate huge fortunes out of the high cost of living, the wages of hunger, excessive prices and rents.

Foreign trusts, such as refrigeration and other North American plants that monopolize the market and the manufacture of general food supplies, must be systematically attacked by the urban guerrilla.

The rebellion of the urban guerrilla and his persistence in intervening in public questions is the best way of insuring public report of the cause we defend. We repeat and insist on repeating: *it is the best way of insuring public support*. As soon as a reasonable section of the population begins to take seriously the action of the urban guerrilla, his success is guaranteed.

The government has no alternative except to intensify repression. The police networks, house searches, arrests of innocent people and of suspects, closing off streets, make life in the city unbearable. The military dictatorship embarks on massive political persecution. Political assassinations and police terror become routine.

In spite of all this, the police systematically fail. The armed forces, the navy, and the air force are mobilized and undertake routine police functions. Even so they find no way to halt guerrilla operations, nor to wipe out the revolutionary organization with its fragmented groups that move around and operate throughout the national territory persistently and contagiously.

The people refuse to collaborate with the authorities, and the general sentiment is that the government is unjust, incapable of solving problems, and resorts purely and simply to the physical liquidation of its opponents.

The political situation in the country is transformed into a military situation in which the gorillas appear more and more to be the ones responsible for errors and violence, while the problems in the lives of the people become truly catastrophic.

When they see the militarists and the dictatorship on the brink of the abyss and fearing the consequences of a revolutionary war which is already at a fairly advanced and irreversible level, the pacifiers, always to be found within the ruling classes, and the right-wing opportunists, partisans of nonviolent struggle, join hands and circulate rumors behind the scenes, begging the hangmen for elections, "redemocratization," constitutional reforms, and other tripe designed to fool the masses and make them stop the revolutionary rebellion in the cities and the rural areas of the country.

But, watching the revolutionaries, the people now understand that it is a farce to vote in elections which have as their sole objective guaranteeing the continuation of the military dictatorship and covering up its crimes.

Attacking wholeheartedly this election farce and the so-called "political solution" so appealing to the opportunists, the urban guerrilla must become more aggressive and violent, resorting without letup to sabotage, terrorism, expropriations, assaults, kidnapings, executions, etc.

This answers any attempt to fool the masses with the opening of Congress and the reorganization of political parties--parties of the government and of the opposition it allows--when all the time the parliament and the so-called parties function thanks to the license of the military dictatorship in a true spectacle of marionettes and dogs on a leash.

The role of the urban guerrilla, in order to win the support of the people, is to continue fighting, keeping in mind the interest of the masses and heightening the disastrous situation in which the government must act. These are the circumstances, disastrous for the dictatorship, which permit the revolutionaries to open rural guerrilla warfare in the midst of the uncontrollable expansion of urban rebellion.

The urban guerrilla is engaged in revolutionary action in favor of the people and with it seeks the participation of the masses in the struggle against the military dictatorship and for the liberation of the country from the yoke of the United States. Beginning with the city and with the support of the people, the rural guerrilla war develops rapidly, establishing its infrastructure carefully while the urban area continues the rebellion.

Urban Guerrilla Warfare, School for Selecting the Guerrilla

Revolution is a social phenomenon that depends on men, arms, and resources. Arms and resources exist in the country and can be taken and used, but to do this it is necessary to count on men. Without them, the arms and the resources have no use and no value. For their part, the men must have two basic and indispensable obligatory qualities:

a) they must have a politico-revolutionary motivation;

b) they must have the necessary technical-revolutionary preparation;

Men with a politico-revolutionary motivation are found among the vast and clearheaded contingents of the enemies of the military dictatorship and of the domination of U.S. imperialism.

Almost daily such men gravitate to urban guerrilla warfare, and it is for this reason that the reaction no longer announces that it has thwarted the revolutionaries and goes through the unpleasantness of seeing them rise up again out of their own ashes.

The men who are best trained, most experienced, and dedicated to urban guerrilla warfare and at the same time to rural guerrilla warfare, constitute the backbone of the revolutionary war and therefore, of the Brazilian revolution. From this backbone will come the marrow of the revolutionary army of national liberation, rising out of guerrilla warfare.

This is the central nucleus, not the bureaucrats and opportunists hidden in the organizational structure, not the empty conferees, the cliched writers of resolutions that remain on paper, but rather the men who fight. The men who from the very first have been determined and ready for anything, who personally participate in revolutionary actions, who do not waver or deceive.

This is the nucleus indoctrinated and disciplined with a long-range strategic and tactical vision consistent with the application Marxists theory, of Leninism, and of Castro-Guevara developments applied to the specific conditions of the Brazilian situation. This is the nucleus that will lead the rebellion through its guerrilla phase.

From it will come man and women with politico-military development, one and indivisible, whose task will be that of future leaders after the triumph of the revolution, in the construction of the new Brazilian society.

As of now, the men and women chosen for urban guerrilla warfare are workers; peasants whom the city has attracted as a market for manpower and who return to the countryside indoctrinated and politically and technically prepared: students, intellectuals, priest. This is the material with which we are building--starting with urban guerrilla warfare--the armed alliance of workers and peasants, with students, intellectuals, priests.

Workers have infinite knowledge in the industrial sphere and are best for urban revolutionary tasks. The urban guerrilla worker participates in the struggle by constructing arms, sabotaging and preparing saboteurs and dynamiters, and personally participating in actions involving hand arms, or organizing strikes and partial paralysis with the characteristics of mass violence in factories, workshops, and other work centers.

The peasants have an extraordinary intuition for knowledge of the land, judgment in confronting the enemy, and the indispensable ability to communicate with the humble masses. The peasant guerrilla is already participating in our struggle and it is he who reaches the guerrilla core, establishes support points in the countryside, finds hiding places for individuals, arms, munitions, supplies, organizes the sowing and harvesting of grain for use in the guerrilla war, chooses the points of transport, cattle-raising posts, and sources of meat supplies, trains the guides that show the rural guerrillas the road, and creates an information service in the countryside.

Students are noted for being particularly crude and coarse and thus they break all the taboos. When they are integrated into urban guerrilla warfare, as is now occurring on a wide scale, they show a special talent for revolutionary violence and soon acquire a high level of political-technical-military skills. Students have plenty of free time on their hands because they are systematically separated, suspended, and expelled from school by the dictatorship and so they begin to spend their time advantageously, in behalf of the revolution.

The intellectuals constitute the vanguard of resistance to arbitrary acts, social injustice, and the terrible inhumanity of the dictatorship of the gorillas. They spread the revolutionary call and they have great influence on people. The urban guerrilla intellectual or artist is the most modern of the Brazilian revolution's adherents.

Churchmen--that is to say, those ministers or priest and religious men of various hierarchies and persuasions--represent a sector that has special ability to communicate with the people, particularly with workers, peasants, and the Brazilian woman. The priest who is an urban guerrilla is an active ingredient in the ongoing Brazilian revolutionary war, and constitutes a powerful arm in the struggle against military power and North American imperialism.

As for the Brazilian woman, her participation in the revolutionary war, and particularly in urban guerrilla warfare, has been marked by an unmatched fighting spirit and tenacity, and it is not by chance that so many women have been accused of participation in guerrilla actions against banks, quarries, military centers, etc., and that so many are in prison while others are sought by the police.

As a school for choosing the guerrilla, urban guerrilla warfare prepares and places at the same level responsibility and efficiency the men and women who share the same dangers fighting, rounding up supplies, serving as messengers or runners, as drivers, sailors, or airplane pilots, obtaining secret information, and helping with propaganda and the task of indoctrination.

Carlos Marighella

June 1969