

# The PARANOID Newsletter

Because they ARE out to get you.

## Introduction

This is the first issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding father say if they were alive today! How is the government eroding your rights you ask? Through Terrorism and Sex offender scares of course! Today's politicians can pass all kinds of laws that destroy Americans freedom because the average citizen is lazy and stupid.

Don't expect the constitution to save you, its worthless paper. If the constitution was worth the paper it was printed on there wouldn't be warrant less searches and wiretaps, foreigners wouldn't be TORTURED and the FBI wouldn't have the authority to perform Sneak and Peek searches. You do know what a sneak and peek warrant is don't you? Have you ever heard of a National Security Letter?

**Sneak and peek search warrant:** A search warrant authorizing law enforcement officers to secretly break and enter into a persons home or business without the owner's or the occupant's permission or knowledge and to clandestinely search the premises. Any crime including misdemeanors may be used to justify a sneak and peek warrant.

**National Security Letter:** A warrant like document invented as a method of circumventing the Right to Financial Privacy Act in 1978. The Patriot Act permits these NSL's to be issued without consulting a judge, merely a Law Enforcement Supervisor. It is frequently used to obtain private records of Americans' Internet service providers, financial institutions and telephone companies. NSL's contain a gag order that prevents the recipient from consulting a lawyer or notifying the target of the investigation.

NOTE: An internal FBI audit found that the bureau violated the rules more than 1000 times in an audit of 10% of its national investigations between 2002 and 2007. Over 20 of these involved requests by agents for information that US law did not permit them to have.

In fact the FCC, the government department that licenses manufactures of radio products CLAIMS to have the authority to inspect your home without a warrant and ANYTIME. If you have a cellphone, CB radio, or anything else that uses radio waves, the FCC claims it can enter your home at any time to inspect it. Donald Winton, the operator of a CB rebroadcasting an AM radio station, refused to let an FCC official in his house, but did turn off the radio. Winton was fined \$7000 for refusing the FCC official entry into his home. Remember, the FCC official is not a police officer. The fine was reduced to \$225 after he proved he had little income. Fortunately, the best the FCC can do is give you a fine.

This newsletter will teach **YOU** how to protect

Your home and office from illegal searches.

Your gun ownership rights.

Your financial records.

Your home, vehicles, cash, etc.

How to have wiretap proof communications.

Learn how the government is recording your every move and how to stop it!

The first order of business is to “get your mind right”. Take all your thoughts of legal protection, fair play, honesty, good faith, cooperation and throw them right out the window. Now lets start clean with a new set of assumptions about the government.

**The government wants to do the following:**

Control everyone and everything on the Internet.  
Take away the savings of the entire nation through inflation.  
Pump propaganda into your home through biased journalism.  
Scare the entire American population into signing away their rights.  
Permit a MASSIVE inflow of Latino Illegal Immigrants into the US.  
Brainwash and dumb down children in public school and deter homeschooling.  
Take control of healthcare decisions and private medical records in the United States.  
Record every number you dial and monitor every step you take by tracking the E911 GPS in your cell.  
Monitor financial transactions through credit card records, bank records, Currency Transaction Reports, etc.  
Register, ban and ultimately confiscate all privately owned firearms, at least any firearm good for self defense.

**Basic tactics to combat the FBI**

**Safeguard your rights to own a firearm:**

**IMPLEMENT THESE STEPS IMMEDIATELY BEFORE FIRARMS ARE BANNED**

Buy several high powered firearms and bury them in watertight containers in the ground.

Use the gunshow loophole to buy firearms from individuals directly, hassle free.

Buy a substantial amount of ammunition, especially hollow point and specialty ammunition.

Buy high capacity magazines.

Buy mail order black powder firearms hassle free.

Don't have gun products sent to your home address.

Don't be associated or affiliated with any gun ownership organizations.

Don't keep more than one or two guns in your home, keep the cashed away incase the government seizes or bans them.

Use Pelican brand waterproof cases to ensure your guns are safe underground. (Wrap the case in heavy duty trash bags to keep the case clean)

Don't let ANYONE know about your extra firearms or that you are interested in firearms.

Buy Shotgun News magazine to get good deals and hard to find items.

## **Safeguard your computer:**

### **DO NOT USE MICROSOFT PRODUCTS**

Use whole disk encryption such as Truecrypt or PGP encrypt everything on your PC with a strong password.

Strong passwords are completely random, 45 characters or larger, use upper and lower case and symbols.

Never write down your password. Perhaps burying it in an underground container would be acceptable.  
Use software that over writes the unused portion of your hard drive with random information.

Overwriting data makes it impossible to recover forensically, be use to use the 7 pass DOD approved method.

Use the Apple operating system, OS X. Windows is so insecure it must be replaced entirely.

If you must use Windows, use it as a decoy computer which the government can steal and think they got your PC.

Buy hardware encryption from Addonics.com, buslink.com or similar hardware encryption products.

Always use a second layer of software encryption such as PGP or that uses passwords since your 5<sup>th</sup> amendment right will prevent you from being forced to divulge a password. A physical key can be subpoenaed.

Keep confidential information on an encrypted laptop, try to lock it in a hidden safe.

Never leave a running cryptographic system unattended. If the government raids you, they can look at everything.

Always check to make sure there isn't a hidden key stroke recorder plugged into your keyboard.

Communicate securely with bitwiseim.com's encrypted instant messenger. The program allows secure voice conversations, secure IM's, secure file transfers and more! The encryption must be done on your end, never rely on the service provider to encrypt for you like Skype. **YOUR ACTIVITY CANNOT BE WIRETAPPED, NOT EVEN BY THE GPVERNMENT WHILE USING BITWISE – IT IS ALL ENCRYPTED.**

Use encrypted offshore proxy servers to establish a SSL encrypted link or other encrypted tunnel to use the Internet. To your Internet Service Provider it looks like your only talking to one server in a foreign country and are just speaking gibberish. **YOUR INTERNET ACTIVITY IS NOT PRIVATE AND CAN BE WIRETAPPED.** Encryption is your **ONLY** protection against wiretapping and it cannot be broken by the government. Neomailbox.net is a good start.

Consider storing all confidential data in encrypted form on a wireless hard disk that is physically hidden in the walls of your house and using an X10 controller to turn the device on and off. The PC can boot from a small hard disk or DVD linux boot image and then connect to the wireless hard disk. USB wireless hubs can be very useful.

128 bit and especially 256 bit and larger key sizes of encryption are **UNBREAKABLE** if you use **RANDOM 45**

character passwords or longer. Always use a known safe encryption algorithm such as AES, Triple DES, Twofish, Serpent or Blowfish. Never give anyone your password. Rely on the 5<sup>th</sup> amendment to not give it up.

When using strong encryption you must use high security tamper proof seals on ALL your equipment. Polylabel.com has serialized holographic tamper proof seals that are EXCELLENT. If your computer can be tampered with, the next time you type in your password the “bug” will record it and then the KGB can break your encryption. You have to be dumb enough to type the password in after the tampering has occurred.

Always smash and burn a hard disk, CD or other computerized media when discarding it.

Always erase and overwrite or otherwise destroy obsolete or unnecessary copies of confidential information.

Always update your computer with security patches. (Windows update, Apple Update)

### **Safeguard your home against illegal searches:**

Buy high security anti bump locks such as the commercial Medeco lock for the front and back door. Do not use a home version. Medeco keys are harder to duplicate and are extremely lock pick resistant. Pin all your windows.

Scan all paper records that must be kept and store them in an encrypted computer that does NOT connect to the Internet. Burn or shred the originals.

Use a metal container to burn confidential material in, such as a metal wastebasket. If you have a fireplace, place the container inside when burning. If you choose to use a shredder use at least a crosscut shredder, a micro cut is better still. Always stir the ashes when burning paper, adding water makes the ashes disintegrate.

Hide confidential items inside home made hiding spots. A junk VCR bought from the thrift store can become an excellent place to hide your goodies. Put it with your other stereo equipment and no one will suspect a thing. If your tech savvy, build a small computer like the mac mini into the VCR case and its a disguised PC! Just use wireless keyboard and mouse and a HDTV for the monitor. Add “void” tamper seals to complete the disguise.

Be careful about having controversial material at home where it could be found by the government. Pornography, racist literature, gun magazines, unpopular religious material, and all sorts of legal but controversial material should be WELL hidden. Get the book “How to hide anything” by Michael Connor

With little effort and expense, you can hide cash, armaments and even family from the menacing eyes of burglars, terrorists or anyone. Learn how to construct dozens of hiding places right in your house and yard. Here are small hiding places for concealing money and jewelry and large places for securing survival supplies or persons. More than 100 drawings show how to turn ordinary items into extraordinary hiding places.

Also read “How to be invisible” by J.J. Luna and visit his website with discussion forum at [howtobeinvisible.com](http://howtobeinvisible.com).

Learn to use Pelican cases to hide important things in the back yard underground. They are 1000x safer under a little dirt in the backyard rather than being in the house for the government to find.

## **Safeguard your money:**

Invest in gold, silver, platinum and palladium bullion, bullion can be redeemed anywhere for local currency and inflation will never eat away at the price of precious metals. Bulliondirect.com is an excellent place to buy.

Hold most of our cash out side of a bank. Keep your cash and bullion safe and hidden away, rather than keeping all your money in a bank where it can be seized by the IRS, creditors or the government.

Do not use credit cards or write checks! They show how much money you spend, where you spend it and credit cards in particular can give detailed accounts of the things you buy. NEVER USE CREDIT CARDS!

If someone opened up a bank account, say a corporate bank account and kept your name off of the records. You could use ATM cards to withdraw cash and to deposit money into the bank. By using ATM's you can conduct virtually all your banking with a machine instead of a person who would ask for ID.

Prepaid debit cards can be used to make telephone and online purchases safely.

Prepaid cellular phones can be used to prevent invasions of your privacy and can be discarded in an instant.

Use money orders rather than checks when possible. Some organizations like stock brokers don't like getting money orders too often. Throw in some cashiers checks, regular checks from "friendly bank accounts" and other varying payment methods to prevent looking like a drug dealer / money launderer.

Cash checks at a liquor store, be careful that the bank has no real address for you, the government will be able to get whatever information you supply them.

Never move money in any amount that would trigger a Currency Transaction Report. Stay well under \$10,000 when doing business whenever possible, it sets off reports to the IRS.

Set up LLC's to own things for you. The book "How to be invisible" by J.J. Luna explains the very easy process. Your company can own houses, cars, planes, just about anything imaginable. When a police man runs the tags on your car he'll will see your information. When they run the tags on a company car they see nothing but the company as the owner. YOUR TAGS WILL BE INVISIBLE. This can easily be done on just about anything, including utility bills which can be used to track you.

Always keep a little checking account open with a small amount of money in it. It is a thermometer to see if anyone tries to seize your assets. You will be put on notice and it'll only cost you a mere \$30 deposit.

Don't fall into debt slavery.

Do anything you can to prevent giving out a social security number, its the standard way to track you down.

If you can work for cash, can be self employed or work out some other friendly arrangement, do it.

Do everything possible to reduce your taxes, the government uses your tax money to do evil. Mail order / imported cigarettes, rolling your own cigarettes, brewing your own beer / wine prevents the government from getting tax revenue.

Social security is a fraudulent Ponzi scheme, do everything you can to avoid it.

Make a “bug out bag”, a backpack with bottled water, canned food, survival knife, money, matches, clean set of sturdy clothes, etc. designed to hold you for 72 hrs in the event of a disaster. ALWAYS have this bag ready.

Learn about food storage from the Mormons, every member has a years supply of food just in case.

### **Safeguard your privacy:**

Set up a front to receive mail. Use commercial mail boxes, remailers, po boxes, “front locations” and other tricks explained in how to be invisible to act as your official address. Consider paying an RV grounds to receive your mail and act as a home address when your “on the road”. Think “room for rent” for a “front” address.

Never let your true name be associated with your true address. Don't even order pizza with your true name.

Want to start fresh? Move to a new state, change your name in that state and then move again. Don't bother changing your drivers license until your in the final state. Also consider that Arizona has drivers licenses that only expire on your 65 birthday!

**Random tip:** Need to visit a doctor confidentially? Visit a doctor and pay cash, use a fake name and give false information for everything. Noe of the information is necessary if your paying cash, especially the social security number. Cash patients don't need that bit of information. Get checked out and never give out your true identity. Filling a prescription is also completely hassle free, WORST CASE if you have trouble, mail order the prescription next day or two day. You can also ask the doctor for free samples of the medicine you need.

## **What to do if the police want to talk to you**

"GOOD MORNING! My name is Investigator Holmes. Do you mind answering a few simple questions?" If you go to your door one day and are greeted with these words, STOP AND THINK! Whether it is the local Police or the F.B.I. at your door, you have certain legal rights of which you ought to be aware before you proceed any further.

In the first place, when the law enforcement authorities come to see you, there are NO "simple questions". Unless they are investigating a traffic accident, you can be sure that they want information about somebody. And that somebody may be you!

Rule number one to remember when confronted by the authorities is that there is NO law requiring you to talk to the Police, the F.B.I., or a representative of any other investigative agency. Even the simplest questions may be loaded and the seemingly harmless bits of information which you volunteer may later become vital links in a chain of circumstantial evidence against you or a friend.

### **DO NOT INVITE THE INVESTIGATOR INTO YOUR HOME!**

Such an invitation not only gives him the opportunity to look around for clues to your lifestyle, friends, reading material, etc; but also tends to prolong the conversation. And the longer the conversation, the more chance there is for a skilled Investigator to find out what he wants to know. Never open your door to an Officer. They can shove their way in. Don't open your door with the chain-lock on, either. Police are known to kick in doors. I should add, that when you let a Police Officer into your house, then he is automatically authorized to do a weapons search (supposedly for his own protection) and this can lead to all kinds of problems!

Many times a Police Officer will ask you to accompany him to the Police Station to answer a few questions. Often, the authorities simply want to photograph a person for identification purposes, a procedure which is easily accomplished by placing him in a private room with a two-way mirror, asking him a few simple questions, and then releasing him. NEVER agree to go to the Police Station. Simply say, "I have nothing to say."

If the Investigator becomes angry at your failure to cooperate and threatens you with arrest ... STAND FIRM. He can't legally place you under arrest or enter your home without a warrant signed by a Judge. (There are exceptions to this however, as in instances where he has witnessed you commit a crime, and there are times, too, where he can enter without showing a warrant up front, known as a 'no knock' entry.) However, if he indicates that he has such a warrant, ask to see it. We've heard of Cops waving a piece of paper around, claiming it was a warrant. A person under arrest or located on the premises to be searched, generally must be shown a warrant if he requests it, and must be given a chance to read it.

Without a warrant, an Officer depends solely upon your helpfulness to obtain the information he wants. So, unless you are quite sure of yourself, don't be helpful. (Note: Don't fool yourself into thinking you can talk or lie your way out of the situation. Don't be smug and think, "All Cops are stupid" and you can pull a 'fast one.' Most Police are smart individuals, they're good at what they do, and the only thing you will do is talk yourself into jail.)

Remember, talk is cheap! But when it involves law enforcement authorities, it may cost you, or someone close to you, dearly. Remember the 5 words -- "I HAVE NOTHING TO SAY." It has worked for us many, MANY times. And it will work for you! There is never, ever, a situation where talking to the police can HELP you. In court any favorable statement to law enforcement is considered hearsay and is inadmissible.

## Security seals offer serious security.

Have you ever tried to open up a computer system with a warranty sticker sealing the removable cover to the frame? As soon as you opened the computer case the warranty seal separated with the repeating text "VOID VOID VOID". Considering the impracticality of brute forcing strongly encrypted files, anyone serious about getting your files will look for another way; hardware tampering is the easiest and most common way to defeat password based encryption systems and capture text. Think of file encryption as a vault door, if you want any real security you have to prevent anyone from breaking in through a glass window.

Holographic Security Seals deter anyone from opening your equipment and alert you if your equipment has been tampered with internally. If your equipment is compromised an attacker could install hardware without your knowledge that is designed to capture your keyboard text or some other input or output that has been decrypted, thereby bypassing the encryption.

The best seals have serial numbers. Some are translucent and others are opaque. We recommend using more than one type security seal so it would be harder for an attacker to counterfeit, lift, cut, chemically dissolve the binding glues or otherwise attack the seal. Seals cost the attacker time and usually hardware tampering is done secretly on site. Every extra minute spent in your office increases the risk of discovery to your attacker. While some may consider this to be excessive security, the cost of seals are only a few dollars. If your serious about having secure equipment they are a requirement. The only real world way to beat strong encryption is to cheat and install key stroke recording devices or otherwise tamper with the systems hardware.

Security seals on computer equipment are rather uncommon and will completely surprise your would be

spy; I would be very surprised to hear of an attack where the spy brought chemical solvents and lifted multiple seals on the first entry. I expect the number one attack on seals to be thin razor cuts. If you aren't careful in your examination you can easily miss a fine razor cut exactly along the seam of the equipment, other attacks are simply failure prone or are impractical to perform outside the lab setting under ideal conditions.

I recommend you place a two different kinds of seals on each part of the case. Ensure that you cover the front, back and sides with seals. After securing the machine make sure you cover the keyboard. There are websites devoted to selling keyboards of every make and model and they have key logging chips inside. In fact, there are even used keyboards to complete the subterfuge. Seals (with serial numbers) do more than prevent them from being opened, they prevent substitution.

Cables can be marked distinctively with an UV pen. Although I am unaware of any attacks being performed against the cabling, it's cheap insurance. In fact you can sign the seals with a UV pen. The ink dissolves on contact with many solvents and represents an extra layer of discrete security. You can verify the authenticity of your equipment with a simple UV LED and it can be used to prove the equipment is yours should it be stolen.

Be sure to examine the keyboard connectors on the keyboard and computer system to ensure an attacker has not secretly installed a keystroke recording device between the cable and the system housing. Keystroke recording devices are a serious security risk and you should check for their presence regularly.

PS. The DOD actually considers a good holographic serialized seal as tamper evident as a very high quality lock that would cost hundreds of dollars!

## **Threats you never thought existed but are still easier than Cryptanalysis.**

The following are some real world extreme attacks against hardened systems. Generally, the only way to defeat string encryption is to cheat. Hiring a cat burglar to put a key logger on a computer is infinitely easier than brute force cryptanalysis. Also bribing someone \$50,000 for the keys to your encryption would be a tremendous savings compared to cryptanalysis of the 128 Bit Triple DES and AES military grade ciphers commercially available. Interestingly enough nearly everything on this list is rendered moot if you

- Keep your secure computer offline (Apple machines are excellent), use a different one for the Internet, this is called an air gap. A hidden away encrypted laptop is 1000x more secure than leaving controversial written material for the government to find.
- Use strong password based software encryption.
- Use strong hardware token based encryption.
- Put tamper seals with serial numbers on all hardware and (ideally) lock the computer in a safe.
- Use high security Medeco brand locks on the door to your computer room. (prevent sneak ins)
- Check for hidden transmitters ("bugs") in the room you operate in.
- Work in a room that doesn't have a window.

- Burn hard disks, CD's, backup tapes before discarding them.
- Laptops are best because they are EXTREMELY portable and easily locked in safes or hidden.

## **So what COULD “they” do?**

### **In order of likelihood**

Break in (or barge in) and secretly (or blatantly) copy the data from your hard drive (or steal the hard drive) onto a portable hard drive and sneak out (or walk out) with a copy of your data to read plain text or analyze for weak passwords, etc. Also looking for sticky notes with passwords on them, etc. This attack is devastating and extremely successful. This is the number one attack performed by private investigators, hackers, law enforcement and spouses.

Replace your keyboard with a bugged version which appears identical but saves everything you type on a chip. This attack is devastating and extremely successful. This is the number two attack performed by private investigators, hackers, law enforcement and spouses. The bugging devices are inexpensive and commercially available.

Install or trick you into installing trojan horse and virus software can secretly transmit data over the internet or disables software encryption. It is believed that the FBI Cyber knight program is designed to capture keystrokes, including passwords to encrypted files, file and other private data. This attack is a real threat, software designed to compromise Windows based PC's is freely available on the commercial market.

Take discarded CD's and Hard Drives out of the trash you set outside on the curb.

Put a hidden video camera where it can observe your monitor. This attack is devastating and extremely successful. This is a common attack performed by private investigators, hackers, law enforcement and spouses. The bugging devices are inexpensive and commercially available.

Listening to the different sounds made when striking different keys on the keyboard and using spell check software to error check. This attack has been performed in the field by intelligence agencies against typewriters since the 1970's at least. Graduate students have released source code permitting anyone to exploit this security issue.

Putting a transmitter in your monitor / keyboard. This is a practical attack for anyone who can substitute or open up your computer hardware.

Trojan horse and virus software that secretly transmits data via the LED's on your keyboard. This attack is not known to have been performed in the field, currently this is a demonstrated hypothetical attack.

Passively reading the data from blinking LED status lights on computers, printers, etc. This attack is not known to have been performed in the field, currently this is a demonstrated hypothetical attack.

Actively transmitting data via TEMPEST signals (computer generated electronic radio noise) out of your computer after a virus or trojan horse program compromises it. This is a demonstrated hypothetical attack. There is even a free program that will play music that you can listen to via AM radio. (see Eliza for Tempest)  
NOTE: Tempest attacks are rare and difficult to perform.

Passively listening to electronic "noise" that comes out of your pc. (TEMPEST) These attacks extremely rare, require very special equipment and require the attacker to be physically close by. These attacks are only performed by federal agencies in major cases, usually foreign espionage. Operate in a metal box (faraday cage) to defeat this attack. Working on a laptop in a closed shipping container would offer outstanding protection. Lookup more information about TEMPEST on the Internet.

**Thank you for reading our first edition**

I hope you enjoyed reading the first edition of the PARANOID NEWSLETTER as much as we enjoyed writing it. We know we just might sound a little out there but think of what George Washington would say if he were alive today! The government is corrupt, evil and is constantly playing the "Terrorism" card to pass illegal laws. We need your support to continue operating. The Newsletter in paper form is always five pages printed on both sides. This is the weight limit for first class mail, priced at .44 cents. If you give us your email address we would be happy to give you the newsletter at absolutely no cost. Since it's free to send it we'll pass the savings on to you! If you are a real supporter of our work however, please ask where to send a donation anyway because we need to get the message out and sending first class mail to potential readers does cost money.

Are you a low tech person? Want the newsletter in paper form? A fifteen dollar donation will keep you in a years supply of the newsletter. We would really rather give it to you in the email format, its a lot less work and expense. You probably have a lot of specific questions and we would be happy to answer them the best we can. Send us an email and your question will be answered and included in the next newsletter. If you would like to buy anything we mention, please email us and we will give you an exact point of contact for the product.

It's not an accident that you received this newsletter. For whatever reason, we believe you would be interested in our newsletter. This is the only copy you will receive unless you contact us. Please pass this information on to everyone with the intelligence to appreciate it.

**Tremendously valuable resources**

<b>Resist.com</b>	<a href="http://www.ncmilitia.org/spycounterspy/">http://www.ncmilitia.org/spycounterspy/</a>
<a href="http://Howtobeinvisible.com">Howtobeinvisible.com</a>	<a href="http://www.backwoodshome.com/articles2/wood115.html">http://www.backwoodshome.com/articles2/wood115.html</a>
<a href="http://www.martykaiser.com/report~1.htm">http://www.martykaiser.com/report~1.htm</a>	<a href="https://thementalmilitia.com/forums/">https://thementalmilitia.com/forums/</a>

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier to any donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the " \_ " character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**

# The PARANOID Newsletter

Because they ARE out to get you.

## **Introduction**

This is the second issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. Today's politicians can pass all kinds of laws that destroy Americans freedom because the average citizen is lazy and stupid. Learn to operate under police state conditions and you'll manage to stay under the radar.

*So it is said that if you know your enemies and know yourself, you can win a hundred battles without a single loss. If you only know yourself, but not your opponent, you may win or may lose. If you know neither yourself nor your enemy, you will always endanger yourself. - Sun Tzu*

*What good fortune for government that the people do not think. - Adolf Hitler*

*An oppressive government is more to be feared than a tiger. - Confucius*

## **Fun facts and thoughts on firearm forensics.**

### **Frustrating the ballistic fingerprinting of firearms.**

Use a caliber conversion kit to confuse the enemy. How can a .45 ACP pistol be responsible for a crime involving a .22 slug found at the scene? Caliber conversion kits usually replace the entire top half of a pistol. A new firing pin, extractor, barrel. etc. this is important because it changes every part that comes into contact with the ammunition. A .45 using a new "top half" is 100% ballistically different from its original configuration. In fact, investigators would be completely convinced that firearm was completely unrelated. In fact, that firearm WAS used... just with a caliber conversion kit.

Black powder revolvers can be mail ordered with no paperwork and no questions asked to anywhere. Pay with a money order and it can be shipped to a P.O. Box no problem. Conversion cylinders convert these black powder firearms to fire modern centerfire ammunition. Two great manufacturers are the kirst conversion cylinder and the R&D conversion cylinder. The Ruger Old Army Revolver is the BEST black powder revolver for this configuration period.

kirstkonverter.com and fcsutler.com sell the conversion cylinders and cabelas.com sells blackpowder revolvers.

Rifle striations on a slug can tell enemy examiners a lot about the firearm that discharged that bullet.

Colt Firearms are made with a left hand twist.

Smith and Wesson firearms are made with a right hand twist.

Twist rates are difference among different manufacturers. Left hand twist, right hand twist , different calibers, hexagonal vs. octagonal rifling and rates of twist can found on slugs can “disqualify” certain makes and models of pistols based on this information alone. Of course police think your not smart enough to buy aftermarket barrels which can change this data and point away from the actual brand of firearm in question.

Glocks, all 9mm (except .357 SIG) and 10mm calibers use a twist rate of 1 in 9.84. In a few minutes I found replacement barrels with a twist rate of 1 in 16. Changing the stock barrel of a firearm can seriously mislead investigators into thinking they are looking at the wrong firearm right off the bat because an extremely obvious detail like caliber and twist rate is wrong. How often do crack dealing niggers change the barrel on their guns?

Cartridge casings (brass) are easier to identify than bullets. Obviously, bullets are usually severely deformed on impact.

Markings on cartridge casings can be matched to the weapons chamber and breech.

Shotguns firing shot generally cannot be matched to a specific firearm barrel due to the lack of rifling and the random contact the shot makes with the barrel as it is fired.

Changing the barrel on a pistol is usually very easy and can be done by field stripping the weapon. Generally, no gunsmith is needed and the new barrel is essentially a new drop in replacement part.

### **Centerfire frangible ammunition: wounding potential and other forensic concerns.**

Am J Forensic Med Pathol. 1998 Dec;19(4):299-302.  
Kaplan J, Klose R, Fossum R, Di Maio VJ.  
State of West Virginia, South Charleston 25309, USA.

Recently developed frangible ammunition of copper particulate construction in .38 Special, 9 mm, and .223 calibers was evaluated for wounding performance by firing into pigs' heads. The ability to match fired bullets with the corresponding gun was also examined. Results showed that wounds caused by 9-mm and .38 Special frangible bullets were comparable in severity to those caused by regular service ammunition of the same caliber. **The recovered 9-mm and .38 Special bullets demonstrated class characteristics but not the individual rifling marks necessary for bullet-to-gun matching.** High-velocity .223-caliber rifle bullets fragmented extensively within target tissues, causing severe wounding. Radiologic examination of resulting wounds showed images strikingly similar to the lead "snowstorm" picture caused by high-velocity hunting ammunition.

In summary, this means using frangible ammunition allows calibers to be determined but matching a frangible slug to a certain caliber BUT NOT TO A CERTAIN FIREARM. Start buying frangible ammunition designed to shatter on impact rather than traditional ammunition.

Some localities, particularly Maryland, have attempted to build up a large database of "fingerprints"; in the case of the Maryland law, all new firearms sales must provide a fired case from the firearm in question to the Maryland State Police, who photograph it and log the information in a database. The Maryland State Police wrote a report critical of the program and asking the Maryland General Assembly to disband it, since it was expensive and had not contributed to solving a single crime. Subsequently however the database did provide evidence used to obtain one murder conviction at an estimated cost of 2.6 million per conviction.

A California Department of Justice survey, using 742 guns used by the California Highway Patrol as a test bed, showed very poor results; even with such a limited database, less than 70% of cases of the same make as the "fingerprint" case yielded the correct gun in the top 15 matches; when a different make of ammunition was used, the success rate dropped to less than 40%.

Gunshot residue (GSR) is principally composed of burnt and unburnt particles from the explosive primer, the propellant, as well as components from the bullet, the cartridge case and the firearm used. There are authors who use other definitions, such as cartridge discharge residue (CDR) or firearm discharge residue (FDR).

GSR mainly focuses on residues containing lead, antimony, barium.

GSR contamination can be minimized by leaving the site of a shooting IMMEDIATELY. A pistol fired indoors was examined and it was discovered that particles took eight minutes to completely settle after being suspended in the air. (*Forensic Science International*, vol 153, p 132).

Industrial tools and fireworks are both capable of producing particles with a similar composition to GSR. And several studies have suggested that car mechanics are particularly at risk of being falsely accused, because some brake linings contain heavy metals and can form GSR-like particles at the temperatures reached during braking.

Unburned gunpowders can have recognizable shapes, colors, and sizes of grains.

primer residues may adhere to fired bullets and gradually ablate through the path of the bullet. Thus, primer residue may be found in targets or wounds at considerable distance from the muzzle (up to 200 meters).

The cartridge case, bullet, bullet coating, and metal jacket also contain specific elements that can be detected. Virtually all cartridge cases are made of brass (70% copper and 30% zinc). A few have a nickel coating. Primer cases are of similar composition (Cu-Zn). Bullet cores are most often lead and antimony, with a very few having a ferrous alloy core. Bullet jackets are usually brass (90% copper with 10% zinc), but some are a ferrous alloy and some are aluminum. Some bullet coatings may also contain nickel.

Modern gunpowder, or "smokeless" powder, can contain up to 23 organic compounds (FBI study). Nitrocellulose is virtually always present, along with other compounds containing nitrate or nitrogen. One of these compounds, diphenylamine (used as a stabilizer in the powder), can be detected using reagents containing sulfuric acid. (Maloney et al, 1982) Modern gunpowders are also described as "single-base" when the basic ingredient is nitrocellulose and as "double-base" when there is additionally 1 to 40% nitroglycerine added. Hardy and Chera (1979) describe a method to differentiate them using a mass spectrometer.

Lead residues may mimic gunshot residue. Lead residues may be found up to 30 feet from the muzzle, and are always present on the opposite side of a penetrated target.

False negatives result from washing of the hands (when this area is sampled) or by victim wearing gloves. A rifle or shotgun may not deposit GSR on hands.

Latent fingerprints may be detectable on cartridges and expended shell casings. Such fingerprints, called latent because they are transferred via a substance on the skin ridges to an object. On a gun, such substances could include cleaning solvents or gun oils. Usually, the substances consist of perspiration mixed with oils from sebaceous glands. Conditions of increased temperature and low humidity decrease the persistence of

fingerprints. **Brass retains the fingerprints better than nickel-plated materials.**

In general, smaller caliber weapons (.22) yield fewer reproducible characteristics in fired bullets than weapons of larger caliber (.45).

The systems for identification of jacketed sporting rifle bullets use twelve parameters:

1. Identification number
2. Manufacturer
3. Weight
4. Diameter
5. Cartridge
6. Base design
7. Length of bearing surface
8. Color
9. Shape
10. Location and description of crimping cannellure
11. Location and description of other cannellures
12. Miscellaneous notes.

Suicide statistics: Firearm suicide entry wound locations			
Site	Handgun(%)	Rifle(%)	Shotgun(%)
Right temple	50.0	22.9	9.3
Left temple	5.8	3.3	3.7
Mouth	14.5	24.3	31.7
Forehead	5.9	15.7	8.1
Under chin	2.4	9.1	10.6
Back of head	3.6	3.8	1.2
Chest	13.2	15.7	19.9
Abdomen	1.4	1.9	5.6
Other	3.2	3.3	9.9

Contact wounds are found in 97.9% of legitimate firearm suicides.

Contact wounds characteristically have soot on the outside of the skin, and muzzle imprint, or laceration of the skin from effects of gases. Contact wounds of airguns usually lack these features (Cohle et al, 1987).

Intermediate, or close-range, wounds may show a wide zone of powder stippling, but lack a muzzle imprint and laceration. The area of powder stippling will depend upon the distance from the muzzle. (Denton et al, 2006)

Acetone and ethanol are very effective at removing nitroglycerine residue from the skin.

## **Comments from a gunshot residue article written by Robert Allman, Jr.**

### **Persistence of Gunshot Residues**

Gunshot residues deposited on a person are continuously lost as a result of normal activities and as a consequence, it is difficult to generalize as to the period over which the residues would be retained. However, the length of time during which gunshot residues remain on hands and clothing of a firer is an important factor in evaluating evidence. If the residues are retained over a period of days, then gunshot residues found on a person's hands or clothing might have resulted from a firing several days prior to the incident under investigation.

Kilty (46) has reported the effect of hand activity and time on the persistence of gunshot residues found on the hands. Persons who test-fired guns had their hands examined for antimony and barium at various timed intervals after shooting. The shooters' activity was unrestricted after firing, except that hand washing was forbidden. This study led to the conclusion that 2 hours after firing, substantial amounts of antimony and barium were removed. Importantly, the same worker (46) reported no evidence of gunshot residue deposition remaining on the hands of a shooter after the hands were washed with soap and water and then dried with paper towels.

Activities shown to remove substantial amounts of antimony and barium include rinsing the hands under low-pressure aerated water for 3 s, wiping the hands on clothing, and placing the hands in pockets three times. In this study, a significant amount of primer residue still remained on the hands of the shooter after placing their hands in their pockets three times. A transfer of antimony and barium from the shooting hand to the non-shooting hand was noted when hands were wiped with towels following a shooting and when the shooter was handcuffed with his hands behind his back and then transported in an automobile. It has also been reported that nitroglycerine residues on the shooter's face, throat, and hands may be retained up to 7 hours (35). For unwashed hands of suicides, deposits may be present for 48 hours and perhaps for a much longer period (18).

A contradictory result has also been reported by Douse (17). In this author's study, no nitroglycerine was detected on hands 0.5 hours after 11 test firings carried out with a variety of weapons and ammunition. The persistence of gunshot residues on cloth is much greater than that on skin. In test firings which were carried out with a revolver, nitroglycerine, nitrocellulose, and diphenylamine have been detected on a variety of clothing types, 6 hours after the firing had taken place. A jumper removed just after firing and stored, undisturbed, was found to retain readily detectable amounts of gunshot residues when examined the following day. No gunshot residues could be detected on the firer after the same time period. This suggests that the loss of gunshot residues is due to physical disturbance rather than any chemical degradation (41). It is further reported that the residues deposited on a cotton sheet placed one metro from a revolver which fired five shots, remained detectable for a period of two months providing the sheet was undisturbed during this period (41).

Lloyd (35) reported that nitroglycerine could be detected on garments which were worn with unrestricted activity for as long as 5 days after test firing. Whether or not the prolonged persistence of the residues on clothing is of value depends on the availability of firearms in the relevant community. Clearly, much greater significance attaches to the results if access to firearms is restricted.

## **Removing serial numbers from firearms**

(Pretty damn accurate comment pulled off the net)

If a person grinding serial numbers off metal really wants to obliterate the numbers and all trace of them, apparently "stress relieving" through annealing is necessary. Heat the thing up to a temperature that I don't know (specific to the alloy) hold it there for a while, and let it cool, and apparently the crystal structure of

the metal de-stresses, and the serial number is no longer available to metallurgists. The gun may no longer be strong enough to use, and will have severely oxidised unless this heating is done in a vacuum, but what the heck, no serial number.

**Yes, annealing is an effective method of preventing forensic recovery of serial numbers from metal surfaces once the number has been defaced.**

The following is taken from a police manual:

### **Methods Used to Obliterate Identification Marks**

1 Filing or grinding- The original number would have been filed away or ground with a power grinder followed by polishing and then over stamping with a new number.

2 Peening- This involves hammering the surface with a round punch to hide the number.

3 Over stamping- Here a new number is simply stamped over the old. For numbers with curved surfaces i.e. 2,3,5,6,9 and 0, the stamp 8 is the one most often chosen. For numbers with straight surfaces i.e. 1 and 7, the stamp 4 is the obvious choice. Serial numbers with a preponderance of '8' or '4' numbers should be treated with suspicion.

4 Centre punching- The surface bearing number is obliterated with a pointed punch.

5 Substitution- Substitution of an iron plate with a new number over the original surface by pasting or welding.

6 Drilling- It removes the number and the surrounding metal with a drill. The cavity is usually filled up with either lead solder or welding material.

7 Welding- Heating the surface with either an oxy-acetylene welder or an arc -welder until the metal flows.

8 Occasionally an original finish would be given to a previous obliterated number surface

### **Chemical etching method for restoration**

The chemical etching method is the simplest and most effective method for restoring obliterated numbers. It is simple to apply and it requires no expensive equipment. It works well on any size or type of object. The techniques involved require considerable skill and great patience. The materials used are potentially dangerous and should be used with full awareness of health and safety requirements. They should only be used in areas specially set aside for this purpose. Rubber gloves will protect the hands from corrosive acid and when using volatile liquids work in the open air away from any seat of naked flame, if laboratory conditions are not available. In case of motor vehicles remove the engine from the vehicle if necessary for ease of access to the engine number surface, and for better quality of photographs of the restoration process.

### **Preliminary Examination**

Examine the metal surface after cleaning oil and dirt away, using acetone. Examine the surface with a hand magnifier and see whether any erasure has taken place at all. Look for any disturbance in the pattern at the background. This pattern will be present either in the form of milled marks caused by grinding the surface before stamping the serial numbers, or cast marks produced during the manufacturing process. If it is disturbed, suspect erasure. Even if no erasure is noticed, remove the paint over a wide area around the surface to check whether the portion carrying the chassis number was removed by cutting and substitute for it by welding or pasting a metal plate with a new number<sup>4</sup>. Remove the pasted plate if any, from the original surface by using trifluoroethanol, after recording the original appearance. Remove the welded plate too. Examine the lower

surface for any obliterated marks. Note how the mark has been erased and whether it has been repaired after erasure. See if any digits or parts of digits are visible. Note these down. Examine the surface by carefully adjusted illumination preferably oblique lighting to see the erased number.

For photography, use a single light for striking the surface bearing the serial number at a low angle. Take several exposures, the light being moved in each instant to strike the surface from a different position. Use process film. This method assists to bringing out the faint serial numbers. Identify the type of metal from which the object is made. This is necessary to choose the appropriate chemical etchants.

### **Preparation of surface**

Clean the surface using preferably benzene or acetone to free it from grease or paint. Solvents such as gasoline, commercial paint remover or 50/50 mixture of acetone and chloroform may also be used. To assist the solvent a soft toothbrush should be used to dislodge deposits from the stamped surface.

Hand polish the area to a smooth, mirror like finish or a reasonably smooth surface with emery cloth, or other fine abrasive. Emery paper with coarse grade is used by first removing all scratches, and other gross marks with fine emery. Do not remove more metal than is necessary. **Leave deep scratches.** Examine the surface during polishing, as digits are sometimes revealed during the process.

Clean again the area with a solvent, such as acetone or other grease solvent. Do not touch the area with bare fingers because fingerprints can interfere with the reaction.

Heating- Treat the area with a blow lamp or Bunsen burner. Care should be taken not to over heat. If the metal is heated to red hot, the temperature is sufficiently high to soften the metal and, on cooling, the metal becomes homogeneous and can no longer be differentiated. A useful guide is to heat the metal surface until it is just too hot to touch. The metal should be allowed to cool before etching begins <sup>1, 2</sup>.

Photograph the entire item, and record details of the obliterated area by close-up photography. Use 35 mm camera with a macro lens and extension and a fast film, 400, ISO.

### **Etching procedures on Steel surfaces (Guns)**

Solution 1 : 90gms Crystalline cupric chloride. + 120ml Concentrated hydrochloric acid. + 100ml Water.

Solution 2 : 15% Nitric acid.

Apply the Solution 1 by swabbing the surface for approximately 2-3 minutes with cotton wool dipped in the reagent. Look for any digits revealed and record these. Clean the surface with acetone (**not water**). Examine again.

Apply the Solution 2 by swabbing the surface for approximately 1 minute with cotton wool dipped in this solution. Look for any digits revealed and record these.

Continue etching alternatively with Fry's and 15% nitric acid etching reagents until the complete number is visible. This may take up to 2 or 3 hours. A consistent check should be made on the appearance of the mark since faint marks appear and then disappear again before the mark is completely etched.

### **Notes:**

- 1. If etching results in areas of dark contrast surrounded by metal with normally etched appearance, this indicates that the mark has been "torched" with a welding torch, and further efforts to restore the mark are a waste of time.**
2. When nitric acid reagent is applied after the Fry's reagent, copper is sometimes deposited on the

surface. This does not matter. It can usually be removed by rubbing vigorously with the nitric acid swab, or alternatively, it will disappear when Fry's reagent is applied again.

### **Cast Iron and Cast Steel:**

Apply constantly a 10 per cent solution of sulphuric acid plus potassium dichromate. Action will be slow. Apply constantly the reagent. It may even be necessary to build a wall of plasticine around the number and fill the hollow with the reagent. Remove the solution at intervals, examine the surface, replace fresh solution. Over development results in the obliteration of the restoration.

Restored marks are to be distinct enough to be visualised and photographed, as far as possible. Better visualisation and photography can often be obtained if the etched surface is moistened slightly with etchants. There should be sufficient lighting to view the restored number because of the difficulty to view properly the number especially on the engine and the chassis of the motor vehicle. Portable beam lighting can be positioned to produce low angle illumination across the surface area for viewing.

However, for photography a powerful light source adjusted suitably for catching their images on the camera screen should be available. Flexible powerful fibre optics illuminators are excellently suited for this purpose. A 35 mm camera screwed on a tripod for time exposure will be very useful. A macro lens with extension rings would enable the camera to keep a close distance from the number area and ensure a magnified image on the film. Use a fast film 400 ISO. A photograph with a contrast film (100 ISO) should also be made. Process the negatives in the usual manner. Print on a normal grade paper for normal contrast.

## **Methods for restoration of obliterated engraved marks**

### **Scope**

Identification of articles of plate and jewellery, and common articles like stainless steel and tool steels by restoring the obliterated engraving identification marks.

### **Engraved Marks**

Engraved marks are made on plate and jewellery using an engraving tool and engraved marks on hard metals like stainless steel and tool steels are produced by an electric engraver. All engraved marks are made by removing the metal with the tool. The underlying metal is not seriously disturbed, and no routine guaranteed method of restoration is possible.

### **Methods of Restoration**

Use (HCL) etching methods for restoring engravings on plated articles. Use acidic ferric chloride on chromium plated on brass plate. Use Fry's reagent for chromium-plated on mild steel plate. **Choose an etching solution which preferentially etches the two metals.**

In case of electrical engraving, the instrument heats the metal at the point of engraving, and partially fuses it. If the number has been filed out, polish the surface carefully. The remains of the fused areas reflect light slightly different from the rest of the metal. Therefore, throw a beam of light onto the polished surface and view through the correct angle. The erased number will be seen as a dark shadow on the bright background

### **Preservation of the restored punched and engraved marks**

1. If a mark is successfully restored, it is important that the number is recorded and, as far as possible, preserved. In an attempt to preserve the mark, the area should be washed with dilute ammonia solution to neutralize the acid (if the surface is acid-etched), cleaned thoroughly with acetone and dried. Clear lacquer should then be thickly sprayed over the mark.
2. It is also important to clean up around the mark. Etching reagents are often splashed or dropped over

surrounding parts of the article being examined, and if not cleaned off, corrosion can result.

3. Remember that different parts of marks will appear and disappear as restoration proceeds. A series of records may be required.

### **Methods for restoration of obliterated painted numbers and other marks**

Some number plates consisted of letters and figures painted onto the metal plate. Obliteration normally consisted in painting over the surface with black or other paint and inserting the false numbers. In a similar manner some floral and ornamental designs, registration numbers and some other identifying features all originally made on the painted motor vehicle surface are obliterated with new designs and numbers.

### **Methods of restoration**

**1-** Take photographs the suspected obliterated surfaces before treating it in any manner. Examine the number plate and the vehicle surface at different illuminations, especially the oblique one. The obliterated marks may sometimes be visible.

**2-** Wash away the fresh paint and the fresh number with chloroform or dioxan. Remember that this action has its dangers because the underlying paint and the marks tend to wash away along with the top layer. Try suitable solvents mixtures of solvents at some other place and thus choose the suitable solvent or mixture of solvents for application in the obliterated surface

**3-** Apply the chosen solvents in cotton swabs over the paint surface suspected of being obliterated. Wait till the top layer just swells. Remove this layer carefully by gentle rubbing with cotton. Look for the obliterated marks and record them by photography and detailed notes. Take care that the underlayer is not washed away and removed along with top layer. Use the above procedure to discover more than one obliterated marks underneath

**4-** X-ray shadowgraph- If the article is portable try this method. Best results are possible when the underlying layers are painted with a paint containing heavy elements, such as lead, while the top paint is free from such elements. With the correct exposure the outlines of obliterated marks can be deciphered.

**5-** In the case of number plates where original sticker number is removed or replaced, try specular reflection. Throw an even light on the plate from an angle and photograph the plate from above. The brightly polished areas, which have been protected by the lettering, reflect the light specularly away from the camera. The weathered areas diffuse the light to some extent and some of this diffused light enters into the camera. As a result, the lettering appears black on a light background

**6-** Expose the plate to ultraviolet radiations. If the area fluoresces in ultraviolet light record the appearance by photography. Photograph following the techniques of UV fluorescence photography.

**7-** A photographic records of the restored marks should be made.

## **Thank you for reading our second edition**

Are you interested in getting the next issue of  
THE PARANOID NEWSLETTER?

I hope you enjoyed reading the second edition of the PARANOID NEWSLETTER as much as we enjoyed writing it. Hopefully these tidbits of information will give you the background to start your own research into law enforcement capabilities and suitable countermeasures.

The government is corrupt, evil and is constantly playing the “Terrorism” card to pass illegal laws. We NEED your support to continue operating. Our Newsletter in paper form is always five pages printed on both sides. This is the weight limit for first class mail, priced at .44 cents. Please pass this information on to everyone with the intelligence to appreciate it. We are absolutely dedicated to fighting the government by educating you as much as possible.

Our current goal is to concentrate as much technical information into our newsletter as possible. Everything in this episode was derived from reading police forensics manuals, books and scholarly articles. Some sections were copied in their entirety and some were summarized from reading long passages. We believe this format is the fastest and most useful way to convey these facts and observations.

Tremendously valuable resources

Resist.com	<a href="http://www.ncmilitia.org/spycounterspy/">http://www.ncmilitia.org/spycounterspy/</a>
Howtobeinvisible.com	<a href="http://www.backwoodshome.com/articles2/wood115.html">http://www.backwoodshome.com/articles2/wood115.html</a>
<a href="http://www.martykaiser.com/report~1.htm">http://www.martykaiser.com/report~1.htm</a>	<a href="https://thementalmilitia.com/forums/">https://thementalmilitia.com/forums/</a>

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier to any donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

P.O. Box 401  
Warsaw, In 46581

# The PARANOID Newsletter

Because they ARE out to get you.

## Introduction

This is the third issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding father say if they were alive today! This DELUXE edition of the paranoid newsletter is exclusively dedicated to defeating FBI surveillance techniques. This current topic will continue into our next edition of the Paranoid Newsletter.

"In America, you listen to man on radio. In Russia, man on radio listen to *you!*", - Yakov Smirnoff

"You have such nice things in the U.S.—like warning shots!" - Yakov Smirnoff

## How to detect and avoid FBI surveillance

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.

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.

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

### **How countersurveillance 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.

**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 (cryptonyms) to disguise the real meaning of their communication.

If you observe that you are under surveillance, 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. 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 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. 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. 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.

## 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.

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.

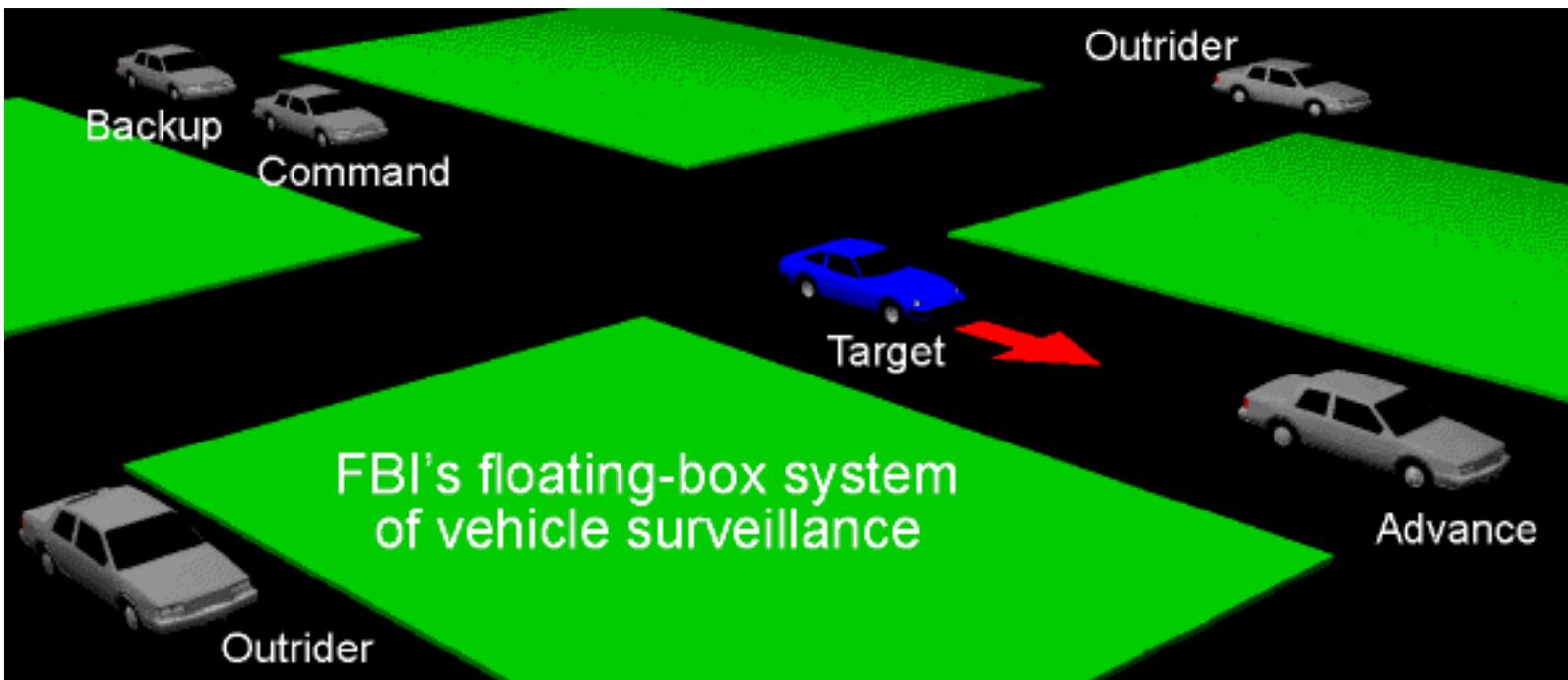
**Floating-box surveillance.** Floating-box surveillance is based on continuous coverage by the same team. FBI agents create a box of surveillance vehicles around you. The box floats with you as you travel along your route. Hence the name floating-box. It is very effective in urban and suburban locations. 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 switches to floating-box surveillance after they have identified general locations where coverage is required.

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, station wagons, 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.

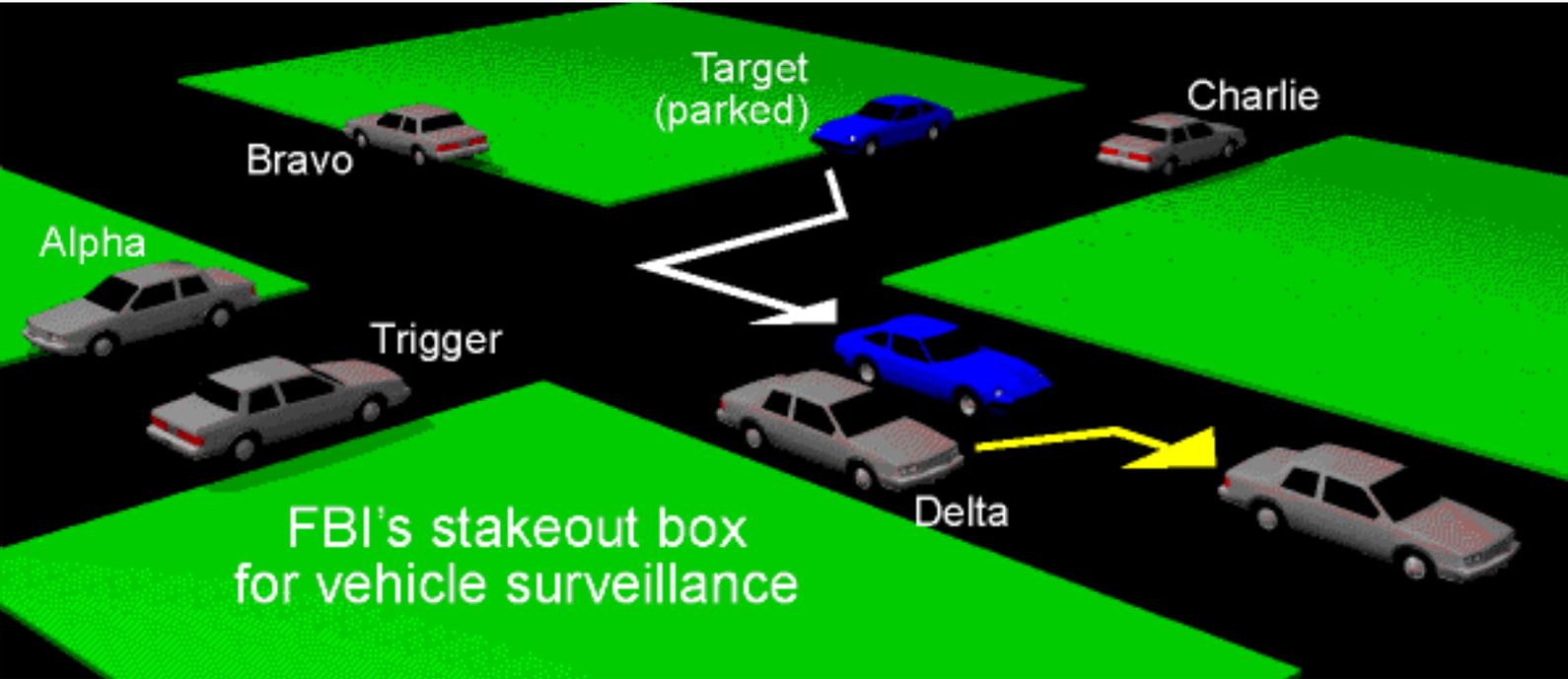
**Recovery from mistakes.** If visual contact with the target is lost, the box can be collapsed inward, enabling the agents to quickly re-acquire *command of the target*. (Whenever the FBI loses visual contact with the target, the surveillance team immediately executes a *lost-command drill*. The FBI 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 practice, a team of five vehicles can be reconfigured  $5 \times 4 \times 3 \times 2 \times 1 = 120$  different ways. Not all of these configurations are useful in the field, especially when the command vehicle's role is unchanged. In practice, 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 than a command vehicle that is following the target.

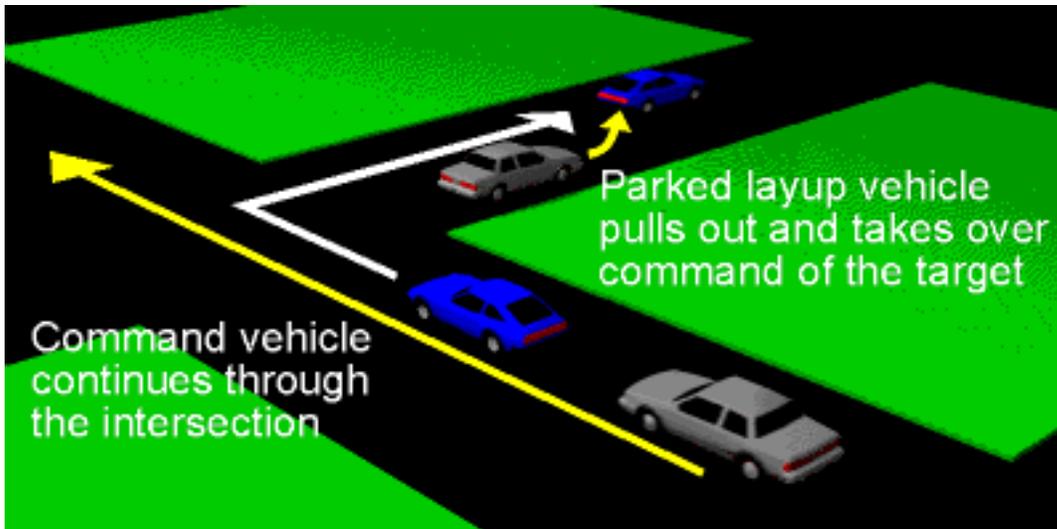
**Command of the target...**

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

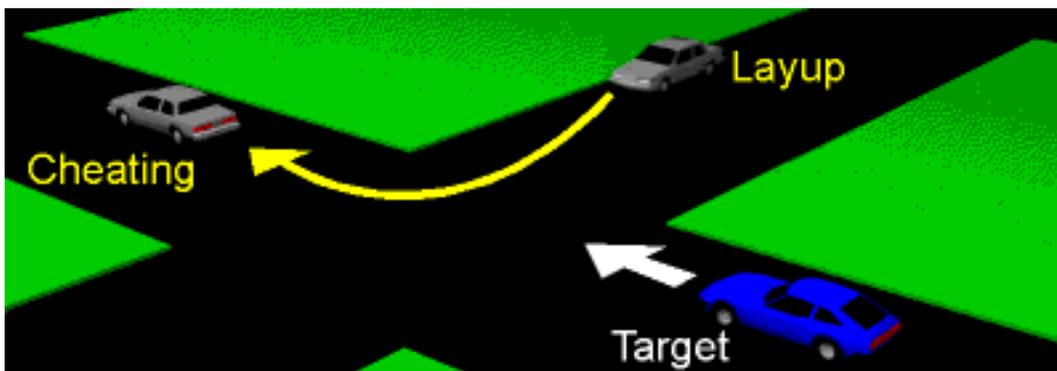
control and power that is provided by this approach is offset by the *vulnerability* of the command vehicle. In many surveillance operations, it is the command vehicle that is first detected by the target. In order to overcome this vulnerability, the FBI has developed a number of tactics to dupe the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



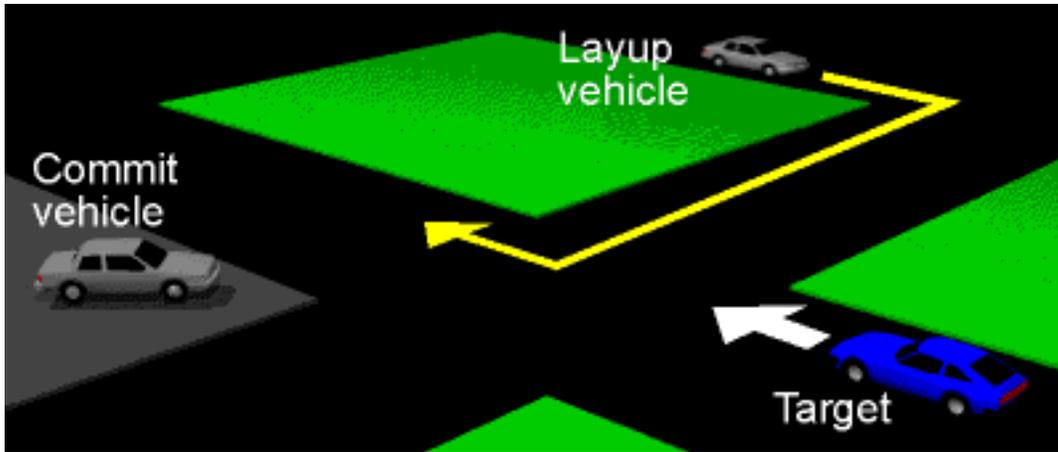
After watching the target make a right turn at the intersection, the *command vehicle* continues straight through the intersection. The agent has, however, alerted one of the *layup vehicles* that the FBI has prepositioned at major *decision points* along the target's route. As you can see from the illustration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

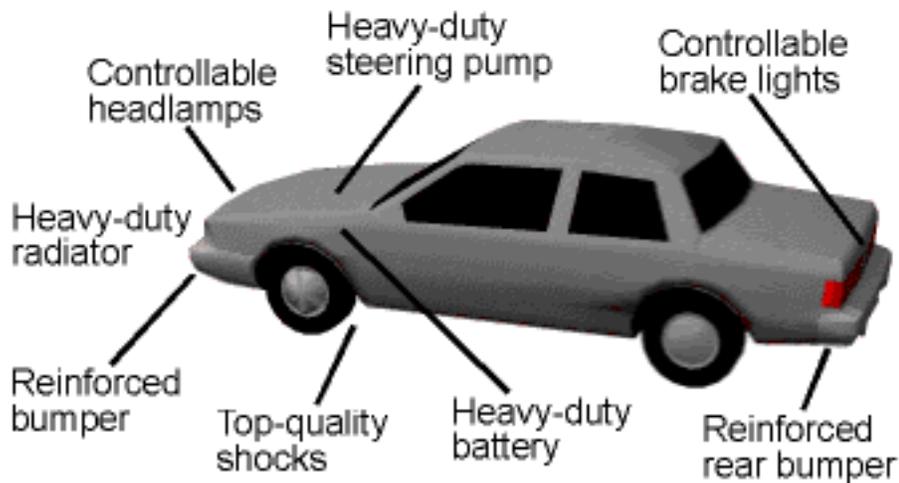


The *commit vehicle* is prepositioned at a major *decision point* along the target's route. The FBI agent in the *commit vehicle* is charged with watching the approaching target vehicle. His assignment is to observe when the target has committed himself to a specific route. Hence the name *commit vehicle*. 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.

## 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*).

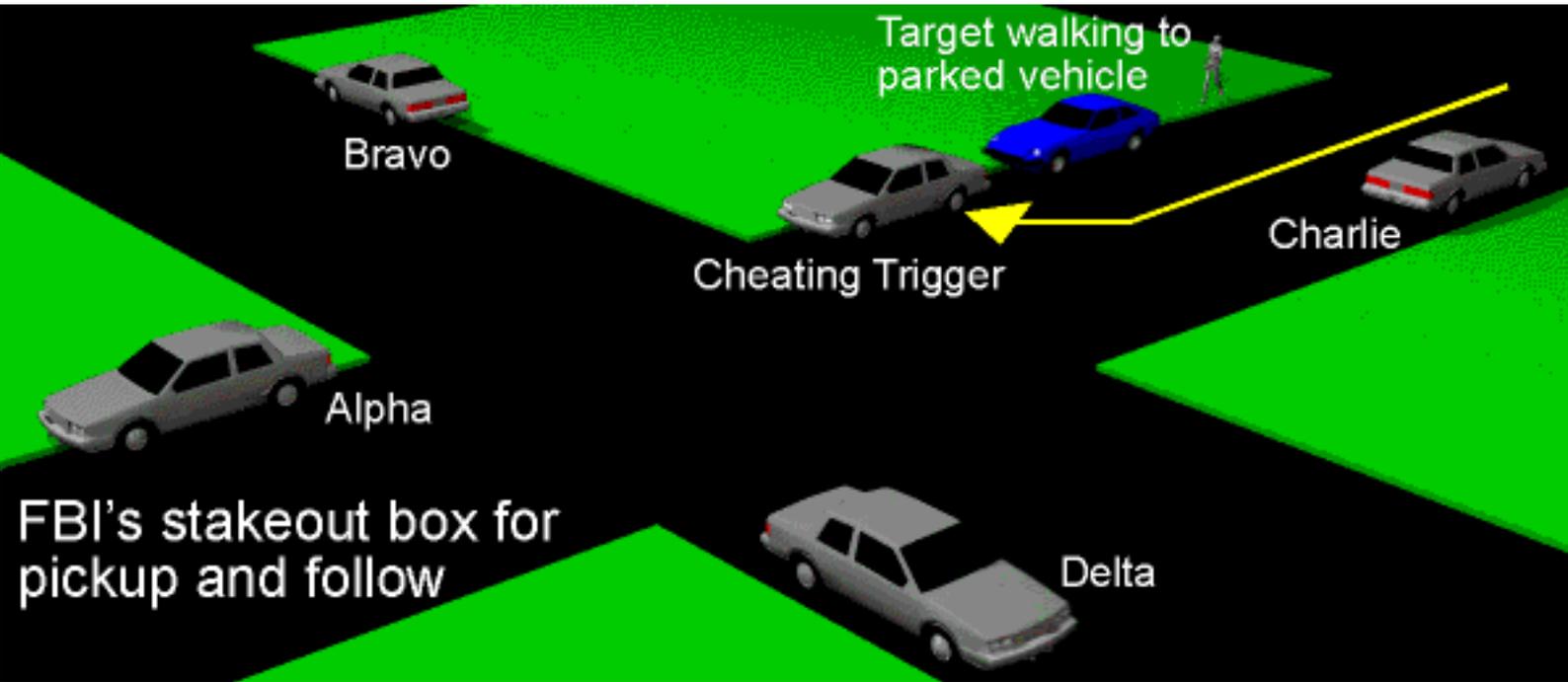
**Controller** – "Is the target *not* in contact with the suspect?"

**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.

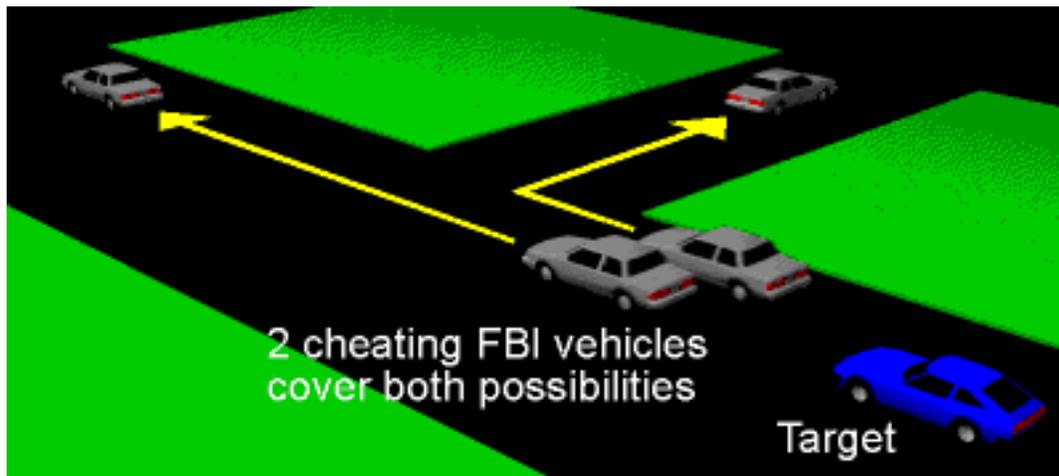
**A common mistake.** If you're like most people, you might be thinking to yourself, "*There's no way they'd use a sweet little sixty-year-old grandmother.*" Yeah, right. Grow up, and stop being such a patsy. The FBI loves *rubes* like you. Or maybe you're thinking, "*No way they'd use a punk rapper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

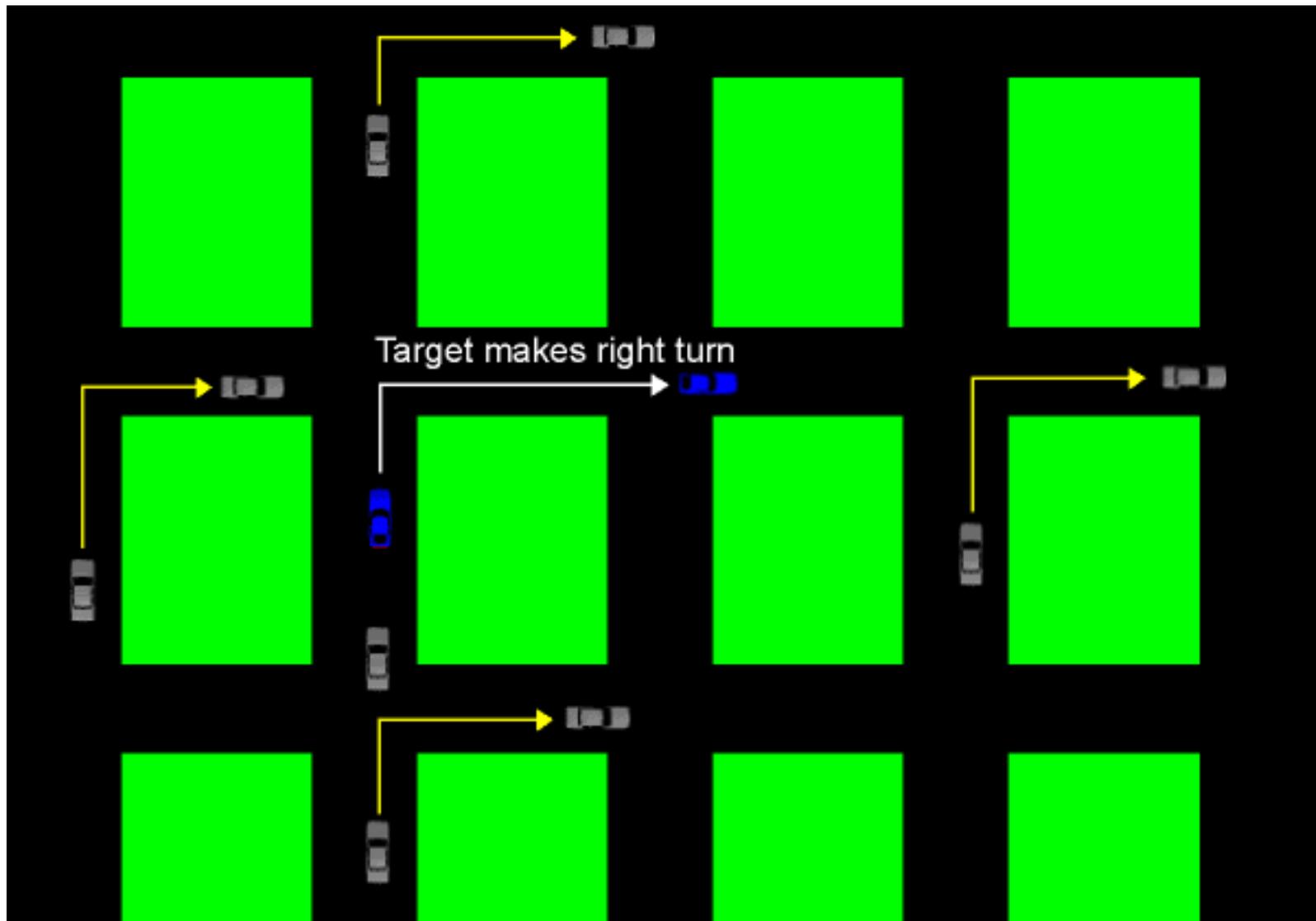
As you learned in the previous article in this series, the FBI utilizes a floating box to track you during a vehicle surveillance operation. The essential components of the box are the command vehicle, the backup vehicle, the left and right outrider vehicles, and the advance vehicle.

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.



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.

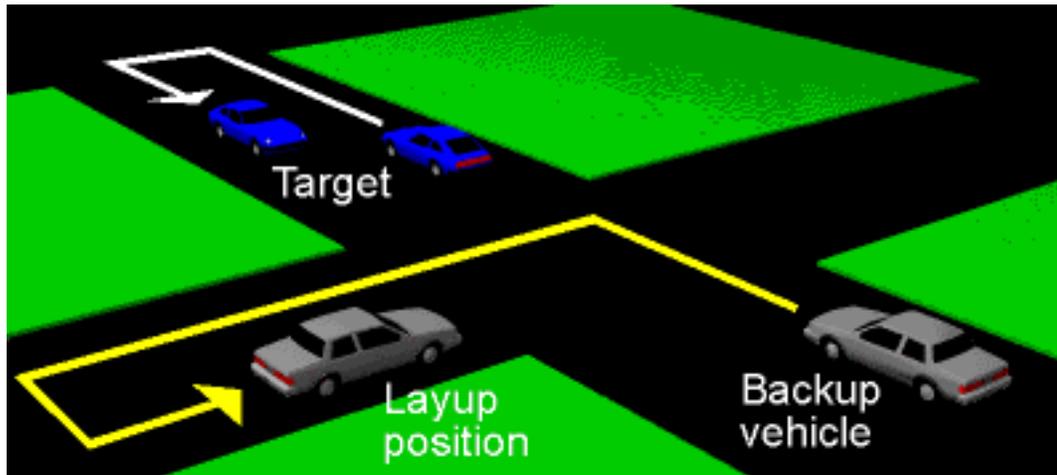


**How a floating box turns.** When the target makes a right turn at an intersection, the right-side *outrider* also turns right – and becomes the new *advance* vehicle. As shown above, other members of the surveillance team also transform their roles. The former *advance* vehicle becomes the new left-side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

## **Thank you for reading our third edition**

### **Tremendously valuable resources**

<b>Resist.com</b>	<a href="http://www.ncmilitia.org/spycounterspy/">http://www.ncmilitia.org/spycounterspy/</a>
Howtobeinvisible.com	<a href="http://www.backwoodshome.com/articles2/wood115.html">http://www.backwoodshome.com/articles2/wood115.html</a>
<a href="http://www.martykaiser.com/report~1.htm">http://www.martykaiser.com/report~1.htm</a>	<a href="https://thementalmilitia.com/forums/">https://thementalmilitia.com/forums/</a>

### **Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier to any donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**

# The PARANOID Newsletter

Because they ARE out to get you.

## Introduction

This is the fourth issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding fathers say if they were alive today! This DELUXE fourth edition of the paranoid newsletter continues where our third edition on defeating FBI surveillance techniques left off. This current topic will continue into our next edition of the Paranoid Newsletter.

Deep doubts, deep wisdom; small doubts, little wisdom. - *Chinese Proverb*

Dig the well before you are thirsty - *Chinese Proverb*

A danger foreseen is half-avoided. - *Cheyenne Proverb*

## Step by step instructions for loosing a "tail"

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. This article teaches you how to check for surveillance before you meet with a clandestine contact. This protocol is generally effective against the FBI, BATF, DEA, and others. This method is particularly effective against standard police surveillance. This method 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.

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. This countersurveillance method has since been adopted as the standard drycleaning method by most intelligence services. 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. We intend for these techniques to become commonplace among insurgents and anti government groups. When this countersurveillance protocol is methodically applied, it is extremely difficult for a security service to breach your security.

Let us assume that you and I wish to meet clandestinely. We wish to ensure that our meeting is not observed by a surveillance team. You and I have previously agreed upon a place, date, and time. In addition, we are familiar with each other's appearance – we can recognize each other on sight.

**Step 1** You and I independently arrive at the previously agreed-upon *general* location. Rather than fixing a specific location, we agree to be only in the *general vicinity*. This is an important principle. This might be a large park, a residential district, etc. The location must be outdoors and free of video surveillance cameras. It

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

**Step 2** You and I will eventually make eye contact at some distance from each other. We do this discretely, so others are unaware. I use a pre-arranged signal to alert you that I have spotted you. Perhaps I'll throw my jacket over my shoulder, or remove and clean my sunglasses, etc. The signal must be a natural movement that does not attract unwanted attention. **Safety first.** Even though you and I have seen each other, we do NOT approach each other. This is an important safety valve. If either of us has *grown a tail* we do not want to compromise the other person. 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 counter surveillance 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.

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 counter surveillance 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. Good 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. American spies call this seven-step protocol for counter surveillance *dry cleaning*.

## 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. Remember, the FBI is in charge of combating professional spies operating in the United States.

The FBI's triple-threat surveillance strategy of *multi-layered teams*, *rapid response*, and *managed aggression* must be taken seriously. Threat number one is 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 number two is the same-day response by the FBI and that means surveillance might begin before you're ready for it. They'll catch you unprepared.

The FBI surveillance team will try to get you under surveillance fast enough to watch you hide the very material that you're hoping to conceal from them. Threat number three is 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.

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 *counter surveillance*. This article reveals some of those methods and techniques. Simply put, the article you are reading is about counter surveillance methods that will beat the FBI.

The FBI are masters of the espionage 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, methodical and thorough. 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. 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.** The concept of multi-layered surveillance teams is the backbone of the FBI's surveillance strategy. They almost never lead with their best team. They always hold something back so that they have a fallback position. This strategy is also carried over into other FBI operations. When the FBI is trying to infiltrate an agent into your circle of friends, associates, coworkers, and acquaintances, they'll often use an expendable agent first. This first agent is a *Decoy Agent*, meant to provide cover for the infiltration by the second agent (the *Stealth Agent*). If the first agent manages to penetrate your organization undetected, the FBI is delighted. But if he runs into difficulty, he is withdrawn. The second agent – who has blended into the background – is brought into play.

**Why the FBI loves your lawyer.** It is important for you to realize that most lawyers have no training in countersurveillance. This is unfortunate. When the subject of an investigation first realizes he is being "followed", he is angry – and outraged at the invasion of his privacy. In many instances, one of the things he'll do is complain to his lawyer about being "followed". Many lawyers advise their clients to "confront" the person who is "following" them. They don't realize that this is a game for foxes, not pit bulls.

The lawyer's advice plays right into the FBI's hand. When the subject attempts to confront the surveillance team, the FBI simply drops back into stealth mode. The Decoy Team suspends its surveillance activity. Because members of the Decoy Team are relatively easy to detect, their absence is easily noticed. The subject assumes that his lawyer's advice has achieved the intended effect. After all, the subject confronted the people who were "following" him and they immediately "stopped". What the subject does not realize, of course, is that the Stealth Team is now active. They have been there all along, of course, as part of the background while the Decoy Team was working. When the Decoy Team departs, the Stealth Team is still there as part of the background. So from the subject's point of view, everything appears to return to normal.

**Basic psychology.** The FBI surveillance team is only too willing to accommodate your emotional desire for control over your immediate environment. It is a fantasy that will lead to your ruin. Here's why. When you see the Decoy Team has departed, you begin to feel safe, so you let down your guard. You become easy prey for the Stealth Team. Of course, infiltration comes next – FBI agents penetrate your circle of friends, associates, coworkers, and acquaintances. Arrest and indictment are simply a question of time.

**Dummy up.** Here's what this means in simple language. You can play the macho man OR you can beat the FBI. You cannot have it both ways. It is an "either-or" situation. If you insist on being a *know-it-all* tough-guy confronting the people who are "following" you, the FBI is going to play you like a cheap fiddle at a country hoe-down. To beat the FBI you need self-control and self-discipline. Be smart. Learn from the mistakes of others. FBI surveillance teams do not just go away. You don't stop wrestling a gorilla when *you* get tired. You stop when the *gorilla* gets tired.

**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. 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. The FBI's capability for same-day response has caught many surveillance targets unprepared. This is not a game for slowpokes. If you don't move fast, you're gonna be roadkill.

**Managed aggression.** This is the third component in the FBI's three-pronged strategy of multi-layered teams, rapid response, and managed aggression. The FBI has a bureau-wide policy of managed aggression. This policy also affects FBI surveillance operations. Surveillance teams are given specific goals. The FBI command

structure accepts no excuses. It tolerates no failures. This strategy of surveillance-for-results leads to aggressive behavior in FBI surveillance teams because of the pressure they're under. This results-driven aggression tends to manifest itself as professional aggression.

An FBI surveillance team is using professional aggression when it intentionally and deliberately applies pressure to the subject of a surveillance operation. Actions like this are called *psy-ops*, which is spy-talk for psychological operations. Here is an example of how an FBI surveillance team will deliberately provoke you. When you're walking through a mall or a downtown shopping district, the surveillance team will intentionally interfere with your route. A pavement artist will "absent-mindedly" cross your path, forcing you to change course to avoid walking into him. A group of agents will "inadvertently" obstruct your path – they'll be standing together chatting, forcing you to walk around them. Other pavement artists will "accidentally" create near-misses as you walk along. Some of these "pedestrians" will create situations with a potential for a head-on collision, forcing you to dodge them.

As the psychological pressure continues to build, agents may "innocently" bump into you, jostle you, or step on your heel from behind. A group of pavement artists will cue up ahead of you, creating a line-up that delays you as you try to make a purchase, order fast food, buy tickets, and so on. Activity like this can quickly create frustration, even anger, in you. But because the incidents occur in public locations, it's difficult to prove who's behind them. You never see any agent more than once. You don't know where the next provocation is going to come from. You're beginning to get upset, irritated, unstable. You're more likely to make mistakes in judgment. And that's exactly what the surveillance team wants.

When a surveillance team is experiencing difficulty cracking open an investigation they sometimes resort to professional aggression. This is a wicked mind-game. It can be very effective if you're not anticipating it. The FBI surveillance team has the power to make or break your day – and they don't hesitate to use that power. This is not a game for choirboys.

**Conclusions:** 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:** 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. In order to strengthen his counter surveillance 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 counter surveillance 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 counter surveillance in an adversarial environment.

**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.

### **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. However, 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. He chokes. Big time. He doesn't know anything about programming. Or computer languages. Or applications. Absolutely zip. Nuttin' at all.

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. 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 counter surveillance.

**Thank you for reading our fourth edition**

**Visit Resist.com to buy future and archived editions.**

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**

*...Where have all the  
SKINHEADS gone?*



# The PARANOID Newsletter

Because they ARE out to get you.

*A fool and water will go the way they are diverted.* - African Proverb

*Not to know is bad, not to wish to know is worse.* - African Proverb

## **Introduction**

This is the fifth issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding father say if they were alive today! This fifth edition of the paranoid newsletter continues where our third edition on defeating FBI surveillance techniques left off. This current topic will continue into our next edition of the Paranoid Newsletter.

## **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. ...

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 articles in

the paranoid newsletter, 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.

### **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. Unbeknownst 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 naive *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 like 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 contacts 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. Use dead drops. Use anonymous email accounts. Use one-time pads. Learn to recognize the warning signs of surveillance. Use elliptical conversation. Use diversions and decoys. Use misinformation. Use codewords. 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.

**Case Study #2.** 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. My cover was that of a naive *dandy* who was hopelessly infatuated with a "*bad girl*".

**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 enforcement 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.

## Comments on Weeding out informants and agent-provocateurs.

**Assessing the risks.** It is imperative that you run tests to verify the reliability and integrity of new recruits 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 recruit 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 recruits. 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.

**How to 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.

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. 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. Punishment ranges from revoking his membership to revoking his birth certificate.

## How to setup a dead letter box

Traditionally, deep-cover agents pass messages, documents, money, weapons, and other material between each other without compromising their security using dead letter boxes. 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. A dead-letter box (British English) is also called a dead drop (American English). 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: Give the ready-to-fill signal.** 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.** 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.** 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.** To maintain watertight security for your DLB, simply weave a number of *fake* DLB locations into your routine on a daily, weekly, or monthly basis. Narrow passageways between buildings, covered pathways in public parks, nearby dumpsters behind restaurants... all these are ideal. Simply make it a point to walk past these fake DLBs *on a regular basis*. Remember, each DLB is located such that you'll be *momentarily hidden from view* as you pass it. If you're under surveillance, the goons will go ballistic. They'll need to place an agent at each suspected DLB *at the precise moment you walk by*.

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

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

# Anonymously and instantly move money via reloadable debit cards

( How the hi tech teenagers and computer nerds move money instantly )

Reloadable debit cards are debit cards that can have funds applied to them at future dates. You need an identity to get the actual plastic card activated. You should also have a safe mail box to get the card mailed to. Pretty much, you go into a store that sells the reloadable debit cards with a bunch of cash in hand. You give a clerk the money, and they give you a temporary card. The temporary card can't be used for much, it is just a number on cardboard, not actual plastic. You need to call and give an information (SS#, address, etc.) to activate the card, and then the actual plastic card is mailed to you.

To activate the card, you should clearly not use an info that has ties to you. You also should not use a phone that has ties to you. Disposable prepaid cell phones are good for this. Also, you should have the card sent to a box registered with a fake ID, or an abandoned house or some such thing. Naturally, there should be nothing to connect you to the debt card.

Although you need a secure place to receive the plastic card, it is very easy for people to send you money. They merely need to go into a store that sells reload packs, and hand the clerk some cash for one. The clerk loads the cash onto the reload card. Now, they can take the number off the reload card and send it to the person with the plastic card. The reload number should be sent encrypted in all cases, in the event law enforcement is monitoring your communication. You do not want to get a persons card flagged, nor do you want to draw attention to yourself.

I suggest people refuse reload card information that is sent to them without encryption. The person with the plastic card can now take the number of the reload card, and can use it to apply funds to their plastic card online. This should be done behind anonymous proxies in all circumstances! Green dot reloadable cards are only sold in the USA, but different countries are likely to have different reloadable cards. Parts of Europe, including Russia and I believe Germany, have Web Money Cards, which are like a mixture between reloadable debit card and E-currency.

When cashing out money from a reloadable debit card at an ATM, a great deal of care can be taken. Gloves should be worn, as should hats and long sleeved clothing. The plastic card should be free of fingerprints, some ATM machines can 'grab' cards, which could later be forensically analyzed. You should park at least a block away from the ATM you use, a better bet would be to use a taxi and be dropped off a block away from the ATM you plan to use. **ALL ATM MACHINES HAVE HIDDEN SURVEILLANCE CAMERAS INSTALLED.**

There are creative payment schemes can be created reloadable debit cards. Someone trusted with access to lots of identities and boxes can get cards in bulk, and resell them once they are activated. People buying pre-activated reloadable debit cards do not need safe boxes or access to identities, they just need a magstripe encoder and blank card stock. Here is the scenario:

One person gets many activated reloadable debit cards. They use a skimmer to get dumps of the magstripe information. Skimmers are usually used by people who commit credit card fraud. Essentially, they

make a perfect digital copy of the information on a cards magstripe. The person can take this dump and encrypt it to a customers encryption key, then encrypt the card dump. The person buying the activated reloadable debit card then decrypts the dump and uses a magstripe encoder to encode it to a blank card stock. The blank card is essentially the activated reloadable debit card now, as far as an ATM can tell.

For this system to work, the person selling the activated card information must be trusted to not keep a copy of the card themselves. If they keep a copy of the card, they could steal money intended for you. If they are trusted and destroy their copy of the card after selling it, this can be a good market for people with access to identities and boxes, and a great way for people to buy anonymous ATM cards that are easy to fund for customers.

Reloadable debit cards should be split up over regions. Time should be allowed to pass between funds being added and money taken off them as well. Remember, reloadable debit cards are not designed for money transfers they are designed to be used as actual debit cards. If the company providing the reloadable card sees it is being loaded by people over a wide area, and the money is immediately cashed out at an ATM, they will likely freeze the card and the assets loaded to it. For this reason, I suggest you use specific reloadable cards to cover different regions of the area you work. Also, if you only work regionally, reloadable debit cards can be the perfect solution. You should not move more than around \$1,000 a month through a single reloadable debit card, or you risk it being frozen.

## **Don't forget to remove the hidden info stored by digital cameras in JPEG images.**

Modern digital cameras encode information about the camera in the jpeg images they create. The first thing we will discuss here is Metadata. Metadata is quite literally data on data. There are various forms of metadata, and it can reveal a lot of information you are probably wanting to keep secret. Let's say you take a picture with a digital camera, and then load it to your computer. If you use the JPEG format, a lot of information is going to be available in your picture. Such information will likely include some or all of the following:

Camera manufacturer, camera model, camera serial number, software used, time of photograph, flash status (did the flash go off when picture was taken) and other technical information.

Now a lot of things can be done with this information. If you post a picture, even from behind an anonymity network, it isn't going to be very anonymous if the picture has the serial number of your camera attached to it with metadata. Perhaps you registered the camera for a warranty, and it will not be trivial for law enforcement to find your true identity. Even if you did not register the camera, often times the serial number can pinpoint the store you bought it from, and in some cases you may still be on CCTV surveillance cameras buying it.

Even if the meta data does not contain your serial number, simply leaking the manufacturer and model of the camera can be used as circumstantial evidence against you after you are raided and the camera is discovered. Software used can leak information about your operating system in many cases, which can be used against you in several different ways (including targeting specific exploits, rather than guessing which OS you are using).

Time of the photograph can help a forensic time line of activity be built and presented against you in court. Sometimes there will be a thumbnail of the photograph stored in metadata, and even if you edit the main photograph the thumbnail will stay the same. So perhaps you have a photograph that reveals information on yourself in part of it, and edit that out. With out removing metadata, you could be at risk of a forensic scientist recovering the information you removed from the picture by analyzing the metadata thumbnail. In other words, a lot of evidence can be gathered on you from a simple digital photograph.

There are a few ways you can remove metadata from photos. One way is to load the photo with metadata to your computer, and then view it full size in a photo editing program. Now hit your print screen button on the keyboard, which is usually right after F12. This takes a screenshot of your desktop. Since the full sized photograph was viewable on your desktop, it takes a screen shot of the photograph. You can now cut out the photograph from the full desktop screen shot, and save it. The newly saved image will not have any metadata attached to it, and you can securely erase the old image.

This trick should work for all formats of images. There are various programs that allow for the removal of metadata from photographs as well, which can come in handy if you want to sanitize a lot of your images and don't have time to take a print screen of each one. I do not know of any such programs off the top of my head, but you will find an abundance of them if you look.

You should also know that the blur function of your image editing program is almost certainly inadequate. Forensics can unblur things pretty easily, the algorithm to blur pixels does not use cryptographically secure number generation and as a result, forensic analysts can reverse engineer the blurring. You need to actually go over the identifying marks with a paintbrush or cut them out, at which point you should likely take a print screen of the edited image. Now cut the image out of the print screen and paste it as a new, edited image.

Microsoft Office documents (such as spreadsheets, presentations, text documents, PDFs) are other sorts of files that can have damning metadata. Document metadata often includes:

The name of the account the document was made in

Name of the company the computer that made the document is registered to

The name of your computer

The account names of people who previously worked on the document

Document revisions

Document versions

Amount of time spent editing the document

As you can see, there is a variety of ways that office file metadata can be used against you. If your computer or account is named after yourself (as many people do), then you could very well be publishing your real name when you publish your sensitive documents. Perhaps the location of your place of work can be determined. Chains of custody can be determined in some cases, meaning if you send a document to someone else people who find the document and analyze the metadata can determine it came from you, and also where

you got it from (or if it originated at you).

There are a few things you can do to minimize the damage of office file metadata. First of all, you shouldn't be using a computer or account named after you in the first place, and you shouldn't be using software that is registered to your name. Second of all, you shouldn't ever do sensitive things from a work computer that has ties to you (although cafe computers can in some cases be ok if you are not directly linked to them). Third of all, after you finish creating an office file, or after you get one before forwarding it on, you should copy and paste the information to a new document and securely erase the original. This will remove some metadata (versions, revisions, time editing, previous authors, etc), but not all of it (computer name, account name, company name, etc).

There are also software tools to remove metadata that you should make use of. The program you use will depend on what type of document you are cleaning. Microsoft has a free metadata remover for Microsoft office documents. I imagine it is probably fairly trustworthy, simply because they intend it to be used by lawyers and such to remove metadata that could leak confidential information. You should be able to find a free program to remove metadata from whatever sort of office document you are using, just use a search engine.

One more specific note on PDFs that certain people might find helpful; simply covering words with black boxes usually won't actually erase them. You can highlight them with the mouse even if they are under the blacked out bits, and then paste them into a word document or some such thing. This exploit was used against a US military agency that released a document with confidential information incorrectly blacked out, and lead to leaking of sensitive information. This is similar to metadata, but isn't. Plain text files are the simplest kind of document format and contain no hidden data whatsoever. These files have the ending .txt and they look like typewriter text. Various fonts, bold, italics, etc. are not possible with this format.

Another sort of metadata on your computer is general operating system created metadata. This can include such things as timestamps (file creation data, last accessed, last modified, etc). It is probably not much of a stretch to call information stored by the OS in places such as the registry as metadata either. Such information can include a great deal of things you likely would not expect. For example, Windows XP keeps a hidden log of every website you have ever visited with internet explorer since the installation of your computer, it also keeps various other data logs including the names of programs you have launched and the dates you launched them.

There are Windows XP tutorials that demonstrate how to disable to built in Windows XP metadata (forensics) tools. Timestamps alone can be very damaging against you. In addition to helping to form a timelines, they can be used to counter defenses in court. Microsoft goes out of its way to design its operating system in such a way as to leave forensic evidence everywhere! Switch to a difference operating system like OS X (Apple) or one of the various Linux based operating systems. OS X is the easiest for inexperienced computer users. Unfortunately, you will have to buy an Apple computer to use OS X. The Mac mini is the least expensive machine offered by Apple and you can use your existing mouse, keyboard, monitor and other accessories.

Don't forget that most color printers encode microscopic yellow dots into the paper that is printed on. The yellow dots are arranged in a way that is unique to each printer. They reveal the model and serial number of the printer they were printed on. This makes it quite easy for someone to positively connect a printer to a certain printed document. This is done at the request of the Secret Service to link counterfeit money to a particular printer. Printer manufacturers do not deny this. Extensive information on this subject is available from the Electronic Frontier Foundation. <http://www.eff.org/issues/printers>

**Thank you for reading our fifth edition**

**Visit Resist.com to buy future and archived editions.**

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**



# The PARANOID Newsletter

Because they ARE out to get you.

*If you don't have a plan for yourself, you'll be a part of someone else's.*

*He who lives on hope will die fasting. - American Proverbs*

## **Introduction**

This is the sixth issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding father say if they were alive today! This sixth edition of the paranoid newsletter covers sending drugs and contraband via the US Mail.

## **Police now recording cell phone info when they make detentions or arrests.**

The NYPD is amassing a database of cell phone users, instructing cops to log serial numbers from suspects' phones in hopes of connecting them to past or future crimes. In the era of disposable, anonymous cell phones, the file could be a treasure-trove for detectives investigating drug rings and other criminal enterprises, police sources say.

"It's used to help build cases," one source said of the new initiative. "It doesn't replace the human element, like debriefing prisoners, but it's another tool to use that we didn't have in the past." A recent internal memo says that when cops make an arrest, they should remove the suspect's cell phone battery to avoid leakage - then jot down the International Mobile Equipment Identity number.

The IMEI number is registered with the service provider whenever a call is made. That data could allow a detective to match, for example, a cell phone used by one suspect to a phone used by another. There are limits to the data's usefulness - all Chinese-made cells sold in India have the same number and some overseas cells are embedded with fake numbers.

Still, civil libertarians are alarmed by the new policy since normally a warrant is needed to obtain information such as calls made or numbers in an address book. New York Civil Liberties Union associate legal director Christopher Dunn said it appears the NYPD is "taking phones apart to get information" without warrants.

"It's hard to believe they feel there's a real need to take out the battery to prevent leakage," he said. "Instead, it looks like they're doing this to circumvent the warrant process." The cell phone information joins another database of more than 20 million 911 callers that the NYPD has been building. It has paid off.

In one case involving a 911 call, detectives solved a burglary pattern after the suspect left a slip of paper with his cell number on it at a crime scene, Deputy Commissioner Paul Browne said. The phone was disposable so no owner information was available, but police were able to track it to the suspect because he had used it to make a 911 call after he was assaulted. The NYPD started collecting 911 data for incidents involving a police response in 2003. Four years ago, it began putting the information into its new computer nerve center, the Real Time Crime Center.

# Comments on mailing drugs and contraband

## **Q. So who is it better to ship with? UPS? Fedex? USPS?**

To answer this question I will give you some statistics on these courier services. Within the USA, USPS delivers over 100 billion pieces of standard mail, 95 billion pieces of first class mail , 1 billion packages, 900 million pieces of priority mail, and 54 million pieces of express mail. Internationally USPS delivers 830 million pieces of mail a year. Including periodicals and other special mailings, USPS handles approximately 213 billion pieces of mail a year.

Fedex handles slightly under two billion pieces of mail total per year, UPS handles around 5.3 billion a year. USPS clearly handles vastly more mail than Fedex or UPS, and this means that your package has more area to blend into. If every single person in the USA inspected a piece of USPS mail every single day, under half the daily volume of USPS mail would be inspected. USPS handles around half as many pieces of mail internationally alone, as fedex handles world wide.

## **Q. Isn't it a serious crime to use USPS to send drugs?**

It is a serious crime to use any mail service to send drugs. You are risking a federal felony regardless of if you are using UPS, FedEx, USPS, DHL or any other service. Using USPS means you are less likely to have a package intercepted, because there is so much more room to blend into.

## **Q. Are there any other reasons I should use USPS?**

Yes. USPS needs a warrant to open your mail. UPS and Fedex do *\*not\** require a warrant to open and inspect your packages. Although law enforcement technically needs a warrant to inspect UPS or Fedex packages, in practice they do not as UPS and Fedex will in all cases cooperate with LE. The requirement of a warrant to open your packages reduces the chances that your package will be intercepted.

Perhaps a judge doesn't think they have enough evidence to open your package. Perhaps someone who would otherwise open a package on a whim will not open your package because they don't feel like going through the steps of getting a warrant and are going to look for another package they find more likely to have contraband in it.

NOTE: The need for a warrant only applies in USA. If your package leaves the country, customs is not going to need a warrant to open it. Similarly, when a package is entering the United States, customs may not need a warrant to open your package.

## **Q. I know what I will do! I will fill my package with cayenne pepper so if a dog smells it then it will have its sense of smell destroyed.**

This will not work. A dog can smell through the pepper, and it is not going to destroy its sense of smell, unless maybe it rips it out and snorts it. Use vacuum sealed bags to reduce the area a dog can hit on your package in.

## **Q. I hear no one ever gets caught for mailing drugs**

Over a thousand people a year are arrested for mailing drugs. While it is true they are often sloppy and

handling bulk, anyone can get busted. The goal is to reduce risk, not pretend it isn't there.

Secure shipping means packaging and mailing products in ways that minimize risk for all involved. Safe shipping is more than packaging a product to reduce risk of interception, it is also using techniques to avoid liability for the shipper and recipient for any seized products

### **What causes a package to be red flagged?**

The following is a list of things customs uses to screen for suspicious parcels. A suspicious attribute of a parcel is called a flag. A single flag is often not much of a problem, but the more flags a package has the higher the chances it will be intercepted.

### **OFFICIAL USPS Package Flag List**

No return address

Restrictive markings (such as writing "Personal!" on the envelope)

Misspelled words

Poorly typed or written text

Excessive postage

Addressed to an incorrect title

Sent from a foreign country

Sealed with tape

Emits a strange odor (Including masking agents such as coffee, perfume and fabric softener sheets)

Lopsided, uneven, rigid, bulky or otherwise uneven weight distribution

Oily stains, discolorations and crystallizations on packaging

Packaging appears to be re-used

Package looks generally poorly prepared for shipping

addresses are hand written

addresses contain misspelled information (such as names, streets or cities)

Originate from a drug source state

Are addressed as being sent from an individual to an individual

Return address ZIP code does not match ZIP code of the post office the package is being sent from

A fictitious return address is used

List a sender or receiver name of a common type (Such as John Smith)

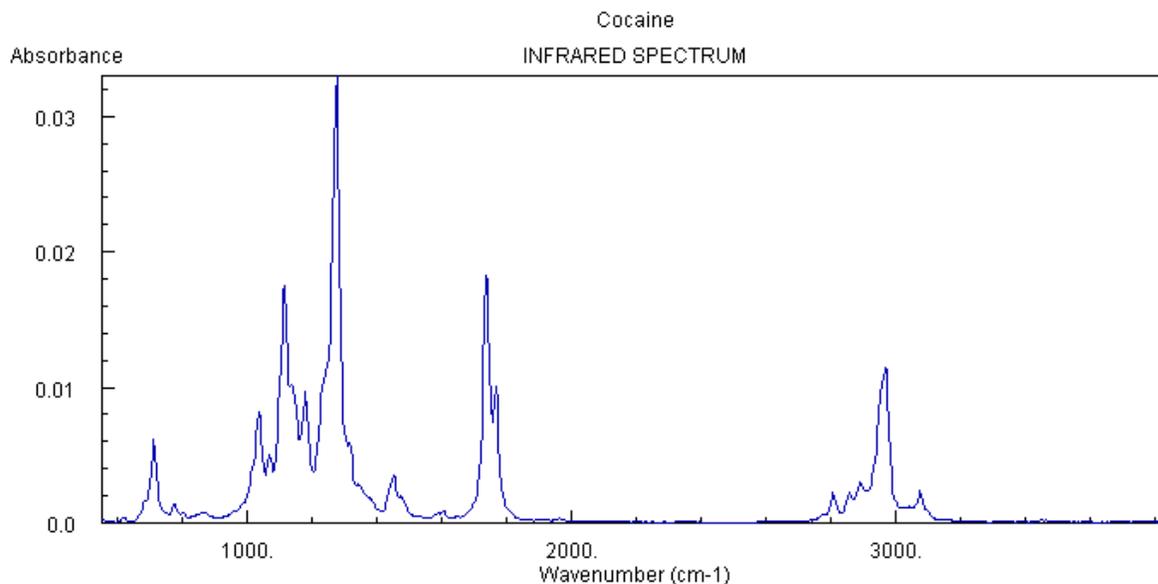
Make use of names that are not connected to either address

Package makes noise when shaken

Redistribution of weight is felt when package is moved or tilted

### **Tera hertz ray scanning**

Illuminating a target envelope with tunable tera hertz radiation and analyzing the absorption spectra of the resulting image. The results are cross referenced with a database of spectra to check for the chemicals of interest.”



Currently it takes ten minutes to fully scan and analyze a single letter, although increasing this speed to one minute per letter is in the grasp of current technology. Even with this potential decrease in the amount of time it takes to scan individual letters, this system could not be implemented en masse without slowing the mail system down to a screeching halt. It is much more likely that this technology will be used to scan mail that has already been flagged by customs personnel using other methods.

Infrared scanners and X-rays work fundamentally in the same way. They are used to detect irregularities in envelopes or packages, which is possible cause for further investigation by other more precise means.

### **Narcotics detection dogs**

Drug dogs are trained to detect even trace amounts of controlled substances in the mail and are used by virtually all customs agencies world wide. Despite their excellent ability to detect certain substances, the overwhelming amount of mail in the system means that they will not be able to sniff all mail. In addition to this, drug dogs are not trained to smell the vast majority of existing psychoactive substances, and due to the staggering number of said substances it is virtually impossible that they ever will be. Using vacuum seals will likely greatly reduce the radius in which a drug dog can hit on a package from, as well as stop agents from smelling products (and avoids masking scents, which as always a bad idea).

### **Drug residue detectors**

“Traces of controlled substances are collected on a small filter held in the end of a vacuum sweeper hose which has been previously tested to insure no contamination. The instrument uses an analytical technique in which the traces of controlled substances on the filter are heated to vapors and ionized. The time required for the ions to drift through an electric field is measured and the substances are identified by the "drift" time through the electric field. ” Below is a picture of an electronic drug detector. These devices can be used to identify many substances. Arson investigators use a similar device to detect accelerants such as gasoline when investigating fires.



## **Substance Identification**

Field agents may test a small sample of an intercepted substance to determine if it is likely an illegal drug (or perhaps confirm it is not what it is documented as). They will likely use traditional reagent tests, such as marquis, to accomplish this. A positive result on a reagent test does not absolutely verify what a substance is, but it is likely probable cause for a search warrant, as it will take some time to get a substance GC/MS tested and they are not usually going to want to tip off a suspect with undue delays.

Absolute identification of a substance will likely be done by GC/MS at a lab. after a package is intercepted GC/MS testing will likely take some time to complete, but is guaranteed to positively identify a substance, provided the lab testing has a reference. Some rare drugs may be difficult for some labs to correctly identify.

## **Evidence Gathering Methods**

Fingerprinting the outside and inside of a package

Handwriting analysis

Analyzing paper and ink

Analyzing type impressions

Forensic analysis of trace evidence (Adhesives, fibers, hair, paint, paper, plastic, rubber, tape, etc.)

Post office surveillance of individuals suspected of sending or receiving drug mail

There are reports of tracking devices being hidden inside intercepted packages when they are being sent to a safe location such as fraudulently obtained PO boxes. The tracking devices then follow the recipient back to their base location where an arrest is later made.

There are reports of people being raided after checking tracking of illegal packages online without using anonymous proxy servers. ALWAYS use an anonymity service when checking your shipping details.

## **Controlled Delivery**

To bust recipients of intercepted drug mail, customs officials will often dress as postmen and make an arrest after the suspect accepts the package. Often times they will allow a few minutes to pass in hopes that the suspect will have opened the package, and then raid the premises. This happens almost always in the case of non-pharmaceutical illegal drug interceptions, and often times with scheduled opiate prescriptions.

## **The "Love Letter"**

Sometimes if you are getting very small amounts of drugs, especially lowly scheduled drugs and pharmaceuticals, you will only get a letter from customs telling you to knock your shit off. They will almost certainly keep your address in a database, so once you get a love letter make sure never to use that address again. A sample of this letter has been attached as appendix A.

## **Surveillance**

You can expect that if you get one package seized, that other incoming packages are likely to be seized as well. So try and only have one incoming pack per box at a time. Also, it is quite likely return address networks can be formed, especially with fast shipping methods. So never ever send mail from a box that has a tie to you unless you get the box JUST for that purpose. Also very frequently change the return address you use to stop network analysis from being done.

## **Packaging Tips for senders**

Use a real return address but make sure it has no connection to you. Frequently change your return address to prevent return address based network analysis. Ensure the ZIP code used is the same one of the drop box you plan to send the package from. A generally sound practice is to use the legitimate address of an apartment complex but do NOT specify an actual number.

The name used should be generic but not overly common.

Keep the front of the package as clean as possible. It should have no markings other than a shipping and return address.

Double check to make sure all information is correct. Also ensure that all words are spelled correctly.

Both addresses should be typed and printed, not handwritten. Ensure the printer used has minimal connection to you (paid for in cash, from a friend, not used for other things). It is easy for forensics to link print to the printer it came from. You may want to use a very cheap printer and dispose of it and get a new one on a semi regular basis (perhaps four times a year).

Exact postage should be applied neatly to the package.

Do not seal the package with tape.

Use self adhesive envelopes and stamps.

## ***Packaging***

Do not attempt to use masking scents, they are completely worthless against dogs, and are a flag to humans.

Double vacuum seal the substance, attempting to spread substance out as thinly and evenly as possible. One method for particularly smelly or sensitive items is to vacuum seal them once, then change gloves to clean pair (you can use tight fitting driving gloves and simply change a pair of latex gloves over top of them), then scrub the outside of the vacuum bag with a light bleach solution. Then vacuum seal the seal bag after it dries *\*fully\** (double vacuum seal).

Ensure that there is no remaining smell of bleach escaping through the bag.

Using super glue or spray adhesive, secure the vacuum sealed bag to a piece of construction paper. Make sure it is secured tightly and that product does not make noises when shaken. Tape should generally be avoided as it tends to add significant weight (especially to smaller orders) and be harder to get a solid stick with. Make sure if you use spray adhesive to be careful not to get dust and such stuck that could be forensically analyzed, although this is unlikely to be a huge issue and anything sticky will leave trace amounts of dusts.

Fold the construction paper over on itself to make it take up as little area as possibly yet still be accommodating for the vacuum sealed bag.

If the thicker cardboard priority envelopes are available, the first envelope should be inserted into one of these. Both envelopes should be addressed.

At all stages of packaging gloves should be worn. Latex gloves should NOT be used by themselves, they are so thin that if any debris (including dust) gets on them, you will leave debris impressions of your fingerprints on what you touch similar to a rubber stamp. Tight fitting gloves made out of cloth or some other material should be utilized. During the stage of packaging where you come in contact with the substance, latex gloves should be worn over the regular gloves. After the substance is vacuum sealed, the latex over gloves should be removed and disposed of before coming into contact with the outer parts of the packaging, to avoid contaminating it with trace amounts of the substance.

Hairnets and long sleeved clothing should be worn during all stages of packaging to prevent hairs from entering the package. Plastic painter suits can be worn to prevent clothing fibers from contaminating the package.

Packages should not be sent from inside post offices but from random drop boxes away from cameras and buildings with cameras. Some care should none the less be taken to disguise facial features and identifying marks.

Keep in mind that the total weight of a package sent via one of the drop off boxes, at least in the United States, is thirteen ounces or less.

The closer to a standard envelope your package looks, the less likely it is to get intercepted.

### **Security tips for recipients**

The best option for recipients it to use PO boxes or PMBs obtained with fake identification. Mom and Pop box companies often have poor security compared to franchises, for example they are less likely to require photocopies of the ID and also are less likely to have a camera system, or if they do have a camera system it is probably very poor as compared to a big franchise company.

Recipients using PO boxes should wait for a lengthy yet random period of time after the package arrives to attempt retrieval. This waiting period dramatically decreases the chances of being apprehended as prolonged surveillance is very expensive.

Disguising efforts should be utilized when retrieving packages (WEAR GLOVES, OR GLUE YOUR FINGER TIPS!), and test runs should also be attempted. (Note: If you are worried about a photocopy of you ID being taken when you open a box, spray hair spray over the face of the card. This will not catch the human eye but will cause the photocopy to be distorted and poor quality. I also suggest if you get a fake ID that you edit your picture slightly in photoshop, slightly change the distance between your eyes and nose. This will prevent someone with a photocopy of your fake ID from finding you by running through the legitimate drivers lisenche database with facial recognition technology).

Do not park near the box place you are using. At the very least park a block away and walk to it. A better plan is to call a taxi from a tracfone and have them pick you up a block away from where you live and drop you off a block away from your box. After you retrieve your package, put it in an anti static bag immediately upon leaving the store. The anti static bag acts as a Faraday cage (make sure the entire package is inside), and will prevent a homing signal from giving your location while the packaging is contained.

Walk to a fast food restaurant or some such thing, and take the package into the rest room area. Go through the packaging and check it for bugs as quickly as possible. Destroy the packaging to the best of your ability and dispose of it (perhaps down the toilet). Now call for a second taxi to pick you up and drop you off a block away from your place of living, and walk back home. It will help to decide the routes you want to take, and the packaging disposal place you want to use, ahead of time.

Another excellent option is to have packages sent to abandoned buildings or houses. The same security methods should be applied as when using a fraudulently obtained mail box.

If a recipient must have a package delivered to a place connected with them, they should ensure said place is clean between shipments. Clean houses of friends can also be used. Upon receiving a package to a place with connections to the recipient, they should not open it but should write return to sender on it. After several days, then the package is safe to be opened. Recipient should NEVER select to have shipping methods which require a package to be signed for.

No matter where you get packages sent, get a feel for the place. Learn to recognize the people that work at your box place. Remember what your mail man looks like. Controlled deliveries are not handled by your traditional mail man, and if a random guy in a mail man uniform asks you to sign something, you should use your head (never sign).

If a friendly neighbor or dude down the street who you never saw before in your life comes by to give you mail they accidentally had delivered to them, make sure you deny it is yours and ask them to just toss it or something. Don't enter the box store immediately, stake the place out and get a feel for the area, see if anyone else is keeping an eye on the place or if it is just you.

Shipping speed is something that needs to be thought about carefully. Sending very fast will rush law enforcements time to obtain a warrant, but will make the package stick out as well. Slow time will make it difficult to determine based on time if a package has been seized or not, but will allow the package to blend in and make it less likely to be seized in the first place. Mail should almost always be sent tracked and never sent with signature.

Recipient will be able to check the status of the package online (use an anonymous proxy server) if it is tracked, and many times the tracking will signal you that the package has been seized (which is excellent to know if it was sent to a fake ID po box you can just drop.) but who knows how long it will take before they notice what is being done and stop announcing on tracking that packages have been seized. I suggest you send messages with a middle level of priority, fast enough that a delay could be noticed but slow enough that the package will not stick out. Try to stay away from both sides of the speed spectrum, but I would say in general slower will be a bit less likely to get seized and faster will be more likely to tip you off if the package is in fact seized.

# DON'T LET THIS BE YOUR HOUSE



Have you ever noticed how police always line up on a door before they force entry? A simple homemade Claymore anti-Personnel directional mine would liquidate all the agents in front of this house.

**Thank you for reading our sixth edition**

**Visit [Resist.com](http://Resist.com) to buy future and archived editions.**

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**



U. S. Department of Homeland Security  
Washington, DC 20229

**U.S. Customs and  
Border Protection**

**Informed Compliance Notice for  
Imported Controlled Substances**



Reference # [REDACTED]

Description: 1 Envelope Containing  
[REDACTED]

Dear Madam/Sir:

This is to notify you that the U.S. Customs and Border Protection (CBP) has interdicted a package addressed to you that contains controlled substances on [REDACTED]. Please be advised that title 21, Code of Federal Regulations, Sections 1312.11 and 1312.12 (21 CFR 1312.1 and 1312.12), prohibit the importation of controlled substances without the express authorization of the Drug Enforcement Administration (DEA).

Unauthorized importations of controlled substances are subject to seizure and forfeiture under the provisions of title 19, United States Code, Section 1595a(c)(1)(B). However, CBP has decided to allow you the option of voluntarily abandoning the property to the Government after which it will be destroyed in accordance with 41 CFR 102-36 at the Government's expense. You may elect to do nothing in response to this notice. If you elect to do nothing, the controlled substances will be considered abandoned after 30 days and destroyed. Finally, you may elect to request that CBP commence seizure and forfeiture proceedings to allow you the opportunity to engage in a formal legal process to petition for the return of the property. Please be advised that no relief from seizure is available unless you are registered with the DEA and have the express written authorization of the DEA to import the controlled substances.

Enclosed is an election of proceedings document. Please indicate your election, sign, date, and return the document to the address indicated on the document. For future reference, enclosed is a public service announcement that warns the general public of the dangers associated with importations of pharmaceuticals. Please note that future attempts to import controlled substances may result in personal penalties or criminal prosecution.

# The PARANOID Newsletter

Because they ARE out to get you.

*"The Yanks have put spectacles on rifles. There isn't no way to avoid a bullet from a mile away."*

*- Letter from a Confederate camp, 1864:*

## **Introduction**

This is the seventh issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding father say if they were alive today! This seventh edition of the paranoid newsletter covers Thermal vision capabilities and methods of defeating FLIR.

**Attention:** Law enforcement officers in the US frequently have one patrol unit on duty with a FLIR camera.

## **Snipers guide to dealing with FLIR equipped adversaries.**

As an electrical utility thermographer, I might shed some light (pun intended) on the subject. To qualify this, I am using the latest (I think) commercially available FLIR product, and am a level II thermographer, (total formal IR training: 2 weeks-experience using IR equipment: about 5 years.) I believe I am at least familiar with IR. Granted, my life is not depending on avoiding IR detection, so I guess I can have my opinions pretty safely. These are my observations about IR imagers using civilian equipment and are.. "just my opinion". It's up to you and yours to check them out in your world.

This is WAY brief, believe it or not. Anyone interested can email for more. This is about THERMAL detection, not IR illuminating sources for "starlight" scopes. IR is not Xray, Hollywood be damned-it cannot detect a differential heat image through common solid materials, plastic film (black or otherwise) being an exception. However, a good imager system can see through holes in a masking material ("IR masking" camo net). If you are inside a dumpster, body heating the bad guy's side, he can "see" the hot spot on the dumpster's outside. But if you are not leaning (heating) against that side, he can't "see you". Your body heat will not be detected behind most readily available unholed blinding materials if you are not differentially warming/cooling those materials or allowing your own IR to reflect off of something behind/over you. BUT, if the shielding materials are alien to the surroundings, the material itself will probably stand out.

Glass will not allow your THERMAL image to transmit (pass) through; same as the dumpster scenario. The lenses of IR imagers are made of exotic nonglass materials because of this. Every piece (cluster) of matter, including gasses, emits IR if it is above Absolute Zero (minus 459.69 degrees F). The warmer a body gets, the more IR it will emit. Eventually it will enter the visible spectrum as it gets "red hot". The surface of a piece of matter is where IR is emitted. Altering an object's surface will alter the rate at which IR is emitted. Stoveblack is a classic example. Materials physically different from each other will likely emit IR at different rates. BUT the differences may be very slight.

IR imaging (read DETECTION) depends upon two objects having one or more differences in Temperature, Emissivity/Reflectivity, and Absorption of the compared objects. For this application, we can forget about Absorption, and you should all understand Temperature. Now,  $E + R = 100\%$ , thus the more emissive a surface is, the less reflective. If two dissimilar objects are at the same temperature, a high E will "look" hotter to an IR imager than a low E, thus forming an image. Objects with different Temperatures and the right E's could "look" the same, thus forming NO image. Two objects with similar temperatures and similar emissivities will present an unclear, poorly defined image. Herein lies your IR strength.

Here are some Emissivity values for a few materials, all in percents, all plus/minus a point or two. These are for short wavelength commercial imagers and may vary slightly for long wavelength/long range military/LE equipment. Military techies should have similar emissivity tables for your equipment.

Human skin : 97  
Black vinyl electrical tape : 97  
Surface sprayed with Dr. Scholl's aerosol foot powder : 96  
Water : 95  
Rubber, black, hard : 94  
Glass, smooth : 94  
Plywood, raw lumber : 90-95  
Most painted surfaces (NON aluminum paint) : 90-95  
Aluminum based paints, depending on formula : 30-50  
Oxidized (blued, parkerized) steel : around 90  
Snow : 82-85  
"Most" organics (vegetation) : around 80  
Cotton loth, untreated : around 80  
Sand : 76  
Clay : 40  
Gravel : 38  
Aluminum, bare and "shiny" (read "spaceblanket") : under 10

Note the materials that cluster around 95, 80, 40, and 10

Now, to apply IR-101: In all of the scenarios below, remember that your body (or ANYTHING above absolute zero) emits IR in ALL directions. If there is a reflective object behind or beside you, it will pick up your IR and reflect it like you were a light bulb. Whichever situation and methods you use, if you have the opportunity, have an ally check you out from a flank with your best IR detection equipment. Or get the flyboys to check you out with FLIR's namesake. Do this by day AND night, as the sun will do weird (but predictable) things to the differential temps.

The BEST way to protect yourself from IR detection is get behind/under what is already there, and DON'T change the temperature of it. Since you obviously have to see and perhaps reach out, do so through the smallest portal(s) you can handle. Those "man-sized" targets detectable at 1100 yards are just that - man-sized - not the size of your nose and right eye. Remember that glass reflects some IR ( $100 - 94 = 6\%$ ), and the sky (space) is cold (approaching Absolute Zero), so if your scope is reflecting not sun, but sky, it will look COLD. If you have on a scope sunshade that is hot, the internal IR of the sunshade will reflect out as HOT.

I believe the New ACU BDU's are treated with an IR emittance reducer. If so, the "cloth" E figure in the table will change and you have to adjust for the following discussion. Or obtain untreated camo fabric or defeat that

treatment (starch, I believe). The IR reducing treatment makes sense for a situation where the woods is cooler than 98.6 F. I hope the Desert Daylight BDU's are NOT treated, but the nighttime anti-starlight smocks probably should be. If your BDU's image "cold" against hot sand, you are just as "seen". I trust the techies were aware of this, and have specified correctly. But you need to confirm by looking through your equipment at your buddy against some typical backgrounds.

It has been reported that "fresh" BDU's do indeed have an IR treatment that fatigues (pun) with laundering in "brightener" detergents. As a hunter, I am aware of the UV problem with animals with good night vision (is it an overabundance of rods, or cones, in the eye?) and there are detergents available via sporting goods stores that do not contain brighteners. If you need to maintain that BDU treatment, you might try that. But again, look at your buddies with your equipment.

Now, in sand or vegetation (E = 76-80): If you HAVE to have artificial cover for situations where your clothing will approximate the temperature of the surroundings, you want to expose matching temperature "stuff" with a similar E (around 80). Cover as much of your skin (97) as possible with cloth (80) (remember that I don't know the E for treated BDU's). But also remember that sweaty cloth in a hot, dry background might look cold due to evaporative cooling. If you are in a hot dry situation, a tented, solid (not net), dry camo fabric applied as a screen might do the trick for IR. (Remember, same T, similar E). Visual is another problem. Keep the outlines irregular for both IR and visual. Square stuff in a curvy world stands out, no matter the technology. Fresh local vegetation in front of the screen will help both.

Camo face paint is PROBABLY a high emitter, similar to regular paints (90-95), and sweat (water-95) is for sure. You really have to keep that face behind something. I don't know what a synthetic ski mask would have for an E, but I bet it is below 97. A plain old cotton tee shirt mask would work, but remember the wet/dry/cooling problem.

Black ANYTHING is a good emitter. Blackened steel barrels, synthetic stocks, and painted surfaces (all E's in the 90's) should be cloth wrapped for IR and visual both. Black SWAT uniforms probably have a higher E than camo. You need to test.

Dry rubber boot soles (94) are nearly as hot as your face - sock 'em (80). Old cut local vegetation will be drier, thus HOTTER due to lack of evaporation. The name of this game is to keep both the Emissivity and the Temperature of the screen and clothing the same as that of the surroundings and keep those portals small. If you are on bare clay or gravel (38-40) and are worried about aerial observation, dig in. Cover yourself with almost anything sufficiently rigid and then cover it with at least a thin but full layer of the local "dirt". This will match the E's. Once the moisture of the new cover layer equals the moisture of the surface around you (evaporative cooling), you will be in decent shape IR wise.

Remember that these low E materials have a high Reflectivity, so block your own IR from getting out from under the cover. If there is a chance your body heat will affect the top surface of the dirt cover, use insulating material between you and the bottom of the "roof" to keep it the same temp as the ground around you. Foam board or sleeping bags will do that. The most critical times of day for this hide would be as the sun changes, because rapid heating/cooling of a thin layer of dirt will show up compared to the slower heating/cooling of the intact soil masses. If you can set up in a shaded spot where this will not occur, you should be in decent shape. If there is no shade, make the cover layer thick to create a heat sink approaching that of the surroundings.

If there is no threat of aerial observation, and it is only a frontal threat, a "wall" of local dirt with small portals would be the best bet. Any new foxhole will print either hot or cold depending on the season and surface temperature, even if the surrounding soil is bare. The deeper soil temp is probably closer to 55 F than the surface. On snow (82-85), build a snow fort or tunnel in and make small portals. Try to dust loose snow to duplicate surface texture. Pray for new

snow. If you wore an aluminized face shield behind that snow fort, it would reflect the "cold" off of the fort, and cover your hot face. This might be a shiny side application of the space blanket, and could be worth testing.

Water (95) is your breath when it condenses. And it is warmer than the snow. Only thing I can think of to do here is breath through a ski mask and let it condense before it fogs up over your screen. As to "**space blanket**" applications: there might be some, BUT. If you are using the shiny side toward you to keep your IR from getting out, remember that the backside of it is probably not a good E match to the surroundings and it will heat/cool a lot differently than most natural things around you. If you are trying to put the shiny side out angled down to reflect the IR of the terrain right in front of you, there would be a 10% reduction in the reflection, more if it casts a shadow. If the shiny side is out and up, it will reflect the cold of outer space (or the heat of the sun) - and it is going to look REALLY weird to visual and starlight in EITHER case! I cannot think of a space blanket application that I would stake MY life on.

In an urban situation, you will have lots of "normal" IR blockers to get under/behind. Just remember that you are an IR light bulb on the cold surfaces behind you. You cannot casually set up back in the room shadows of a windowless building anymore. Remember, glass will NOT pass through (transmit) your IR image. BUT, glass (94) has a high emissivity and will show its surface temperature rather well. If you are near the window warming it with your breath, you will reveal yourself. If you had a small barrel portal through an otherwise intact glass window, you would be IR blocked, but visually seen. A loose pane of glass back in the room shadows might be a possibility, especially for a spotter. If the room is painted (90-95) and warm (approaching 98.6 F), you might blend in IR wise. But if there is one warm window/room in an "empty" building, something is amiss. The painted walls behind you might not reflect your IR really well, but a metallic light fixture might blink every time you turn your face toward it. The best I can imagine is forget about the "room" and get behind/under something that should be there - sofas, chairs, drapes, etc. and keep your portal small.

None of the above CONCEALMENT strategies are easy; none are guaranteed to make you disappear to an imager. But they will all help make you a less vivid IR image, thus less detectable. IR imagers may or may not have an adjustment to key in the emissivity for scanning and reading temperatures. I doubt military/LE targeting devices would have that - you don't care what the actual temp is, you just want to see a picture. Military/LEO devices probably have a temperature range adjustment to scale up/down according to environment. They probably have an adjustment to set the sensitivity - the difference in perceived T to go from black to white (dark green to light green; whatever). If this is finely tuned, it is like upping the contrast on your monitor.

There is one comforting thing to consider: unless you are in the desert, there are a lot of different "things" around you, each of them with a slightly different Temperature and Emittance combination. If you can make yourself "nearly" match the most common IR surroundings and the sensitivity is set very high in order to pick up your small T/E difference, the other guy is seeing a lot more clutter around you, so your image will be just one spot on the Dalmatian. For the Ghillie fans: A man sized wad of only burlap and jute rope at 98.6 F plus or minus a few degrees will have the same E all over it. But if there was some leafage from an IR blocking camo net on one shoulder and a splotch of shredded BDU's at the waist and some foreign force camo material shredded in there somewhere in a cluster, all well supplemented with local veggies, from an IR standpoint it would look like a pile of dissimilar "stuff".

If you have gotten this far, perhaps a little DECEPTION is in order to up your advantage. Remember that "Sarge WILL find something during an inspection, so ya might as well give him something so he will stop looking." If you want to determine if indeed IR detectors are out there, you might want to give them a cowboy hat to shoot at. I don't know what the E of a bare GI plastic canteen is, but if you either wrapped it with Scotch 33 electrical tape (97) from a demo/como kit or sprayed it with foot powder (96) from your ruck, and had 98 degree water (coffee? Body heat?) in it, it would make a darned good human face (97) to a distant IR imager. Topped with a BDU hat and moved

about on a stick behind some intentionally inadequate screening after dark (by somebody else behind that cowboy's large rock), I suspect you would soon know the targeting capabilities of the opposition - and also acquire a muzzle flash.

A piece of most anything warmer than the terrain drug remotely through the grass at night should get IR attention. Just don't pull it all the way to your position. But you get the idea. If you want to just give him/them something to worry about, scatter some old tire shreds (94) around at points distant from your position. They will look hotter than most surroundings when they are actually the same temperature. Plus, they will heat up more during sunlight, and hold their temperature for quite a while into dusk. If you can make them move a bit, so much the better. If they are behind intentionally poor screens, thus not visually or starlight identifiable, so much the better. This would be a great application for decoys specially made for the purpose - a visually camo'd, high E lollipop on a spindly, flexible stick.

One of the new IR illumination chemlights would do something, but I have no experience with them. I suspect one of them tripped off in front of or to the side of your position, yourself in a shadow from it, would blind any thermal imagers looking at you - like a trip flare would blind a starlight. Obviously this would be a defensive action. There have been some pretty impressive demonstrations of the capabilities of IR equipment. And it is indeed impressive stuff, but it ain't magic. It can image warm footprints on a cold roof, or a "ghost" where you leaned against a cold wall and walked away. But those images fade pretty quickly - faster than the grass will spring back up on your trail to a nest.

I believe that if one person takes the time to study and understand the theory of IR systems and applies it to likely circumstances in his world and does it better than the other guy does, the first guy has an EXCELLENT chance of being the winner. That is true for sniping or bidding on a roof inspection. Even an unfavorable tilt in sophistication of equipment may be overcome with intelligent application of ingenuity. And it won't take a lot of formal training. After that, it is experience behind an imager. In your case, looking at your buddies in drill hides, and correcting each other's errors. I grant you that my "thermacam" is not a military targeting device, but if your life is professionally depending on IR avoidance, I hope you have access to IR theory training and support along with the opportunity to drill with your own imagers.

If you may be exposed to a "new" technology, you just have to learn it and apply it. Like you did for visual and starlight. In fact, most of those old rules apply to IR: Irregular outlines. fresh vegetation. local materials. etc. The only real new rule is "Similar E - Similar T". Now, get with some equipment and TRAIN, DRILL, EXAMINE, .

## **Want to buy some FLIR camouflage?**

### **Stealthbag.com**

The StealthBag keeps your heat in for survival and has an aluminized color when turning the bag inside-out to aid rescuers to spot you visually. The StealthBag has "chocolate-chip" desert cammo pattern for Visual camouflage, and still retains radiant body heat so the user cannot be picked up by infrared-seeking instruments.

The StealthBag was tested on a variety of commercial and military-grade infrared detection equipment. The highly regarded FLIR, Inc. Model 2000AB chopper-mounted IR detector (operating in the 8-14 micron wavelength range), was unable during a 30-minute test to locate three individuals inside StealthBags. When the original LAND/Shark was introduced, SOF ran tests with a Life-Finder hand-held IR detector, with similar results.

Weighing less than a G.I. poncho, the StealthBag comes vacuum-packed for long-term storage in a mylar bag, in a 600-denier nylon carrying pouch. After a knife, this is now the first item that gets put in our go pack, for certain protection against whatever elements one may encounter on land, sea or air.

The StealthBag is available at an introductory discount price of \$49.95 plus \$6.99 shipping/handling from Corporate Air Parts, Dept. SOF, 7641 Densmore Ave., Van Nuys, CA 91406-2043; phone: 818-997-0512; fax: 818-997-0478; web site: [www.stealthbag.com](http://www.stealthbag.com) .

## **Comments on FLIR from a Law enforcement discussion board.**

FLIR is a sort of video camera, but it doesn't see visible light; it senses minute differences in temperatures and assigns various shades to them according to what's hottest and coolest. This results in ghost-like images that look reversed, like a photographic negative. What's most impressive is that FLIR can "see" through thin foliage as well as rain and snow-and those capabilities can be just as important in daylight as in darkness.

That would sound like the end of the world to a sniper if there were no means to counter it, but there are. I'm not going to be too specific (bad guys can read, too), [LWDC yes we are reading your manuals and we have our own so FUCK YOU] but I think it's obvious that if you can change your external body temperature or make it close to the temperature of things around you-think of it as another way of camouflaging yourself into your surroundings-then the FLIR won't be able to distinguish you. There's a true story about a Marine sniper gunny at Quantico who purchased an item at a flea market for \$2 [LWDC it was an umbrella you cocksucker] and used it to hide from a multimillion dollar thermal detection system-with several congressmen watching. Yes, FLIR can be fooled.

A thermal detection-resistant Ghillie suit has been developed in Britain that vents and deflects body heat to reduce the wearer's thermal image. I'm not sure how effective it actually is. On this side of the Atlantic, Custom Concealment makes two Ghillie suits specially modified to enhance their resistance to thermal detection. Examining FLIR photos of demonstrators wearing these suits, I don't think there can be any question that the heat signature has been reduced, and quite a bit.

An even more novel approach has been that of a Greek defense contractor, Intermat Group SA, which developed an anti thermal cream. Applied to exposed parts of the body-face, arms, and hands, where heat is registered by a FLIR most easily-the dense cream blocks heat dissipation, thereby reducing the wearer's thermal signature. This is a serious product from a manufacturer that already makes paints serious and specialized coatings for helmets, uniforms, and vehicles to reduce their detection by IR systems. They may actually have something, since all the FLIR images I've seen are brightest at the very spots that this cream would cover. I wouldn't be too concerned about the enemy using FLIR against us since its more of a future threat than a current one. If the day comes that an is a enemy uses FLIR against us, we'll already have the techniques and the technology to counter it.

## **Comments from a FLIR manufacturer.**

How does rain and fog affect the range of my FLIR camera?

A thermal imaging camera produces an image based on the differences in thermal radiation that an object emits. In essence, the farther this infrared signal has to travel from the target to the camera, the more of that signal can be lost along the way. As such, the attenuation factor needs to be taken into account. This is the ratio of the incident radiation

to the radiation transmitted through a shielding material. Humid air acts as a “shield” for infrared radiation. Summer month atmospheres usually have a higher attenuation compared to winter months due to increased humidity levels. Therefore, assuming clear skies and good weather conditions, you will be able to see farther with a thermal imaging camera in winter than in summer.

Humid air is just one example of how infrared radiation can be lost. There are other climatic conditions which are far more detrimental to the range of a thermal imaging camera. Fog and rain can severely limit the range of a thermal imaging system due to scattering of light off droplets of water. The higher the density of droplets, the more the infrared signal is diminished. An important question that customers ask is how much rain or fog will limit the range performance of a thermal infrared camera, and how does this compare to the range in the visible region of the spectrum.

## **Fog classifications**

Fog is a visible aggregate of minute water droplets suspended in the atmosphere at or near the surface of the earth. When air is almost saturated with water vapor, this means that the relative humidity is close to 100%, and that fog can form in the presence of a sufficient number of condensation nuclei, which can be smoke or dust particles.

There are different types of fog. Advection fog is formed through the mixing of two air masses with different temperatures and/or humidity. Another form is radiative fog. This is formed in a process of radiative cooling of the air at temperatures close to the dew point. Some fogbanks are denser than others because the water droplets have grown bigger through accretion. In fog conditions droplets can absorb more water and grow considerably in size. The question whether scattering is less in the IR waveband compared to the visible range depends on the size distribution of the droplets.

There are different ways to classify fog. An often-used classification is the one used by the International Civil Aviation Organization (ICAO). According to this system, fog can be classified in 4 categories:

Category I: visual range 1220 meters

Category II: visual range 610 meters

Category IIIa: visual range 305 meters

Category IIIc: visual range 92 meters

The reason for degradation of visibility in a foggy atmosphere is the absorption and scattering of natural or artificial illumination by fog particles. The amount of absorption and scattering depends on the microphysical structure of the fog particles, which are also called aerosols.

Moderate Resolution Propagation Model (MODTRAN)

MODTRAN is an atmospheric radiative transfer code created and supported by the United States Air Force. It has the ability to model the atmosphere under a variety of atmospheric conditions. It can predict atmospheric properties including path radiances, path transmission, sky radiances and surface reaching solar and lunar irradiances for a wide range of wavelengths and spectral resolutions. MODTRAN enables the calculation of transmittance and radiance in a wide spectral range. It offers six climate models for different geographical latitudes and seasons. The model also defines six different aerosol types which can appear in each of the climates.

Each of the climate models can be combined with the different aerosols. How far you can see through fog or rain with a thermal imaging camera will also depend on the climate in which you are using the camera and the type of aerosol which is present in this specific climate. In general, a comparison of the different aerosols shows that the

maritime aerosols always result in the lowest detection range independent of the climate model, since maritime aerosols have in average greater particle radii than rural and urban aerosols. The rural and urban aerosols produce noticeably greater detection ranges in the infrared band. This means that you can see less well through fog in maritime conditions than in land conditions, irrespective of the climate type.

Just as the type and thickness of the atmosphere has an influence on how far one can see through fog, the type of infrared camera used and specifically the waveband in which the camera operates are also of importance.

There are two wavebands of importance for thermal imaging cameras:

3.0-5 $\mu$ m (MWIR)

8-12 $\mu$ m (LWIR).

**The 5-8 $\mu$ m band is blocked by spectral absorption of the atmosphere by water vapor to such a tremendous extent that it is rarely used for imaging.**

Thermal imaging cameras that are equipped with uncooled sensors are designed to work in the longwave infrared (LWIR) band between 7 and 14 microns in wavelength, where terrestrial targets emit most of their infrared energy and uncooled detection is easy. Thermal cameras that are equipped with cooled detectors (where the sensors are cooled to cryogenic temperatures) are the most sensitive to small temperature differences in scene temperature and are generally designed to image in the midwave infrared band (MWIR) or in the longwave (LWIR) band.

The spectral transmission is different in the MWIR and the LWIR bands. Therefore there will be a difference how far one can see through fog with a thermal imaging camera equipped with an uncooled LWIR detector compared to a cooled MWIR detector. In the LWIR the best conditions occur in winter with low absolute humidity and a rural aerosol distribution. In the MWIR band the detection range is best in conditions with high temperatures, like a summer or tropical atmosphere. All detection ranges for IR are significantly better than the visual for Cat I type of fog. For Cat II type of fog the result is four times better with a thermal imaging camera equipped with a LWIR detector compared to visual.

In Cat IIIa and Cat IIIc types of fog, there is virtually no difference between how far you can see with a thermal imaging camera and with the naked eye since the atmosphere is the limiting factor. Radiation does not penetrate through this dense type of fog in all (visible, MWIR and LWIR) spectral bands.

## **Conclusion & results**

According to these models, Cat I and Cat II types of fog, the thermal IR band offers better range performance compared to the visual band. As such, thermal IR cameras are well suited to look through these types of fog. The models suggest that thermal imaging cameras are potentially useful as landing aids for airplanes or as part of driver vision enhancement systems for the transportation and automotive industry.

The models suggest that fog penetration is higher in the LWIR compared to the MWIR band in all studied cases. For Cat II type of fog, the LWIR spectral band offers about four times better range performance compared to the MWIR band. However, sensor thermal sensitivity and the target signatures must be taken into account to arrive at a final selection of the best system to meet the application. Also cost considerations come into play. For instance, for security & surveillance applications, it is generally not economical to use uncooled LWIR systems for longer ranges as the lenses become too big and expensive. MWIR radiation is adversely affected by atmospheric pollutants and pollutant gases (possible increased atmospheric absorption and/or increase levels of inpath

radiance – both of which reduce target image contrast). LWIR is much less affected.

**Rain can significantly reduce target contrast** (due to increased atmospheric scattering and general obscuration) and LWIR and MWIR perform similarly in the presence of rain. IR system performance degradation due to rain is very range sensitive, whereby there is a dramatic drop off in the 100-500 meter range.

Just like it is impossible to give a simple answer to the question “How far can I see with a thermal imaging camera?”, it is equally impossible to say how much shorter the range will be in foggy or rainy conditions. This is not only dependent on the atmospheric conditions and the type of fog but it is also dependent on the IR camera used and on the properties of the target (size, temperature difference of the target and background, etc)

### **For more information**

Marijuana growers are frequently concerned about FLIR detection of their grow houses. Specifically, law enforcement officers look for heat signatures put off by powerful indoor lighting systems. There are heat shielding products, videos on defeating FLIR, etc. produced by and for Marijuana growers. Look into these materials and products for the most up to date countermeasures. Whether you like drug dealers or not, these people have to worry about FLIR on a regular basis – LEARN FROM THEM.



### **Border Patrol intercepting illegal immigrants crossing the border.**

Notice how “hot” the uncovered face is compared to everything else.



## If you are prepared you can defeat FLIR

Some readers have inquired as to why The Paranoid Newsletter includes so much technical information. Wouldn't it be easier to speak in a general sense about the topics covered? We will never dumb down our publication to appeal to the masses. Instead of dumbing our material down, you will have to bring yourself up to speed. This newsletter consists of concentrated technical information.

In order survive in a high tech society, you will simply have to learn how technology works or you will be left behind. We intend for this newsletter to give you a basic understanding and introduction to the material presented. You will have to do follow up research to understand the subject matter completely. If you do independent research, you will be better prepared than those who seek to use this technology against you. As a small unit or independent operator you are required to have a superior understanding of technology to defeat a large and well funded enemy.

**Thank you for reading our seventh edition**

**Visit [Resist.com](http://Resist.com) to buy future and archived editions.**

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**

# The PARANOID Newsletter

Because they ARE out to get you.

"In Florida, contract murders are refined to an art form.  
The preferred method is two taps to the head with a .22"  
-Former FBI Agent

## Introduction

This is the eighth issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding fathers say if they were alive today! This eighth edition of the paranoid newsletter is written by a former FBI agent. Our anonymous contributor explains the basics of how educated white criminals avoid problems with street cops.

**Educated White Criminals:** Some are white-collar crooks whose swindles fill the newspapers. Others use their scientific knowledge to manufacture designer drugs that addict and kill but are not on the narcotics schedule because of small variations in the chemical formulas. Many of the Dilaudid knockoffs and amphetamine derivatives come from these crooks. The first large shipments of ecstasy, were brought into the United States from Europe by Orthodox Jews when it was outlawed. No one suspected that such educated, pious people could be criminals, so they were able to bring tens of thousands of tablets through airport customs without being searched.

Cops know that rich bad guys are wily and difficult to catch. They generally drive street-legal luxury cars and rarely get searched or arrested, except perhaps for DUI during traffic stops. Almost never are they dumb enough to carry drugs and guns in their automobiles. When anything happens, they lawyer up fast with the biggest and the best. This makes them nearly impervious to arrest by routine policing methods. When is the last time you heard about your police force making an arrest for a complex multimillion-dollar fraud? Generally the federal government tackles the rich guys, and leaves clueless niggers and wetbacks to the local boys and girls in blue.

Real bad guys share one characteristic: they're hard to catch by cops driving around in cars. The only way to catch big crooks without filling up stadiums with petty offenders is the hard way, through more investigations, more undercover work, more paid informants, more phone taps, more hidden video and sound recording. This is tough, expensive, and dangerous, but it's the only technique that nets big fish and results in solid prosecutions with long prison sentences.

*(So don't talk anywhere there could be an electronic device. Don't talk in cars, houses, motels, or even in your favorite table at a restaurant or in the same place outdoors repeatedly. Several mafia dons were caught on audio tape this way. ALWAYS go to a random place to talk after strip searching and metal detecting the other guy. The key here is RANDOM PLACE, the FBI bugged every coin operated parking meter on a city block to catch mafia don who always talked about business outside of his apartment while he walked along the sidewalk. If you talk to someone about important business have then strip down and get into cotton surgical scrubs, exercise jogging suit or something with absolutely no metal. You can't even let people wear their shoes or a hat, both have been used to hide eavesdropping devices. Obviously, watches, cell phones*

*and anything containing metal is forbidden. Electronic recording devices require metal and the easiest way to beat them is to remove all metal then use a handheld metal detector.)*

The biggest criminals share many of the same qualities that bring success in the straight world: intelligence, discipline, persistence, savvy, and the quality of not being clueless. Rednecks have some knowledge of police procedure. They know that police do *not* like to find guns, so they carry the all-purpose and legal knife. When they do carry guns, they are likely to have a permit.

**White Middle-class people are the most exasperating group of crooks because they rarely get caught.** There are two reasons. Even when they indulge in petty crimes and run-of-the-mill thuggishness, middle-class types are harder to arrest and convict because they know the system a bit better. When doing petty crimes, they tend to keep dope at home rather than in their cars and on their persons.

### **Habits of highly successful white criminals**

They grow their own weed and avoid buying it and falling into police traps.

They call cops “sir” rather than “motherfucker”.

They beat women in detached houses rather than apartments, so screams aren't heard and police don't get called.

They make restitution and talk their way out of petty theft raps.

They carry firearms legally.

They sell stolen property to fences rather than peddle it door-to-door in view of police.

They drive street-legal cars, so they are pulled over and searched less often.

They avoid hanging out and living the arrestable, urban outdoor lifestyle (middle-class punks “hang in” and plan and execute crimes indoors, where difficult-to obtain search warrants are necessary to root them out and arrest them)

They read their mail, mark their calendars, and set the alarm so they can wake up, dress up, and show up, albeit grudgingly, at court hearings, probation meetings, anger-management classes, and drug rehab Middle-class thugs, in their scumbag fashion, emphasize the major point of this book. The less clueless you are about the system, the less likely you are to be arrested, even if you *are* a lowlife.

### **MORE IMPORTANTLY: THEY DO CRIMES THAT POLICE CAN'T SEE OR ARE UNTRAINED TO INVESTIGATE.**

Middle-class crooks have long ago discovered the obvious, do crimes where there aren't any cops. Better yet, do crimes that patrol cops aren't trained and equipped to *recognize*, much less investigate. Middle-class whites dominate the following major crime categories: insurance fraud, mortgage fraud, bank fraud, investment fraud, securities fraud, prescription fraud, check fraud, Medicare and Medicaid fraud, embezzlement, identity theft, phishing, Internet fraud, money laundering, manufacturing of phony passports and Ids, mid- and high-level drug distribution, manufacturing and distribution of illegal drugs like Dilaudid, LSD, and ecstasy, fake pharmaceutical drug manufacturing and importation, illegal pornography, counterfeiting of currency, automobile titles, luxury goods, music, movies, and software, immigrant smuggling, high-end prostitution, terrorism, confidence rackets,

extortion and protection rackets, illegal gambling, government procurement fraud and bid rigging, labor racketeering, bribery and vote fraud.

These are enormous criminal enterprises. Thousands of criminals are involved, but comparatively few are arrested. Here's why, all these crimes have one feature in common: *Cops driving around in cars can't see them*. Sounds simple, and it is. No see 'em, no arrest 'em. Think about this. When your local porn king is making unspeakable child pornography videos, what do cops driving around see? A warehouse or office building with some cars parked out front—that's all. Cops can't see through walls so they drive on.

Take bank and mortgage fraud. It happens in offices, cops don't go there. Even if they drive by and happen to see a fraud artist, what do they see? A guy with a briefcase. That's all. Drive on. Furthermore, street cops are untrained to even recognize many of these crimes, even if they do see them being committed. Sound farfetched? Imagine this. A guy is sitting at a table on his front porch committing insurance fraud. He's preparing a phony claim that will net him hundreds of thousands of dollars. This is a major felony. If a cop drives by, what does he see? A guy filling out forms with a ballpoint pen. It doesn't look suspicious, drive on.

Here's another example, a money launderer is sitting in one of those fancy coffee shops where you buy overpriced java and use the Internet. The bad guy is gathering up funds from multiple banks from porn purchases made over the Internet and paid by credit card. This is how kiddie porn is sold. He then transfers the money to overseas banks. All of this can be done with a laptop computer and an Internet account opened under a phony name and paid for with an untraceable cash card. Imagine that a cop walks quietly into the coffee shop and actually looks over the money launderer's shoulder and witnesses illegal money transfers. All he sees is a guy typing numbers and letters on a computer screen. For all the cop knows, the guy is paying his light bill or ordering a movie ticket. No arrest, back to the car, drive on.

Middle-class crime is not small potatoes. The quantities of money are astounding. A middle-class crook perpetrating a single insurance fraud—for example, making a phony disability claim—can make hundreds of thousands of dollars, more than a bank robber could even dream about. For clueless people, the money from crime is hit or miss. Score something here; score something there. There are feast days and famine, but in the end most clueless types who try to make a living from crime end up living in crummy apartments. Sooner or later, they and, generally, their female relatives become impoverished by the criminal justice system, which sucks out their money to pay fines, court costs, attorney's fees, bail bonds, and drug court and probation charges. Middle-class crime is more like a conveyor belt. Enormous quantities of illegal goods and services move outward to the public, and a never-ending pile of money flows back to the crooks. *Ka-ching! Ka-ching! Ka-ching!*

Every day is a payday and the register never stops ringing. The FBI is quite good at investigating middle-class crooks. The methods they use—consensual monitors (“wires”), wiretaps, stings, reverse cons, confidential informants, and undercover ops—are the only way to investigate, arrest, and successfully prosecute middle-class crooks. There are, however, two little problems.

1. FBI agents only investigate federal crimes.

2. There aren't many FBI agents. In my city, for example, there are *thousands* of patrol cops riding around in cars and busting people like you. There are only *dozens* of FBI agents. These days, a huge proportion of bureau resources is dedicated to national security. This leaves middle-class crooks more latitude than ever to keep raking it in.

Cops can't arrest smart white criminals because their resources are grossly misdeployed. Police department detectives can use many of the same investigative techniques as the FBI, but police departments have nowhere near

the numbers of detectives necessary to make a dent in middle-class crime. In any case, most detectives spend all their time, of necessity, investigating homicides, kidnappings, armed robberies, carjackings, and other violent crimes. Often *nobody* is going after middle-class crooks.

Another complication is that middle-class crimes often involve transactions across state lines and national borders and violations of both state and federal law. This means these crimes fall between the cracks of different jurisdictions. Are the cops or the FBI in charge? Maybe the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Office of the Bank Examiner; the Secret Service; the Drug Enforcement Agency; or the Border Patrol should take a hand. Often no one can decide who's in charge. Another interagency task force gets formed, and another SNAFU (situation normal, all fucked up). Ho-hum in Bureaucrat Land.

Police departments are stuck in the last century in regard to their ability to hunt and arrest middle-class criminals. To catch them, police departments will have to become radically different than they are today. They will have to employ, directly or on contract, battalions of the following kinds of people, many of whom can be civilians rather than sworn officers. Many will have job specialties most cops can't even spell:

Fraud investigators, forensic accountants, banking investigators, insurance investigators, securities investigators, phone and communications specialists, Internet specialists, database specialists, computer technicians, data-recovery technicians, encryption/decryption technicians, liaisons to Interpol and federal and state law enforcement, undercover investigators and "sting" operations specialists.

Cops are massively deployed to catch you at the less sophisticated things you're likely to be up to, carrying weed; driving with a suspended license or expired tag; drinking in public; running from cops; fighting with women; failing to appear at court hearings, probation meetings, and drug court; violating parole; and so forth. Cops often aren't even looking for middle-class crooks laundering money; distributing kiddie porn; and perpetrating insurance, mortgage, and Medicare fraud.

Niggers, wetbacks and white trash are hassled by cops right and left, stopped, searched, questioned, and annoyed while all these evil, middle-class perps are stealing money hand over fist with nary a cop around to even slow them down. Their insurance frauds and bullshit lawsuits push up the cost of automobile insurance so you can barely afford to drive street legal. Maybe you can't even buy car insurance right now and have to drive outlaw until the next few paychecks. Sweating bullets every time a cop pulls up on your rear bumper and runs your tag on his onboard computer is no way to live. The system isn't fair. It's just there. Your challenge is to arrest-proof yourself.

The biggest criminals have many of the qualities that bring success in the straight world: intelligence, discipline, persistence, and savvy. They are not clueless. This portrait conflates several actual people in Jacksonville and Miami. I've added a dash of James Bond super criminal as well. Most mid- and high-level drug dealers aren't this smart. They compensate for lack of IQ by blowing out the brains of people who annoy them, such as witnesses.

Lets explore how educated whites commit crime. Our subject, "the chemist," is in his 40s, the holder of a master's degree in chemistry from a prestigious university. He manufactures a high grade of methamphetamine that is sold on the streets under the name crystal lightning. Most manufacturers deliver meth to distributors, who then dilute it for sale at wildly varying dosages with anything from baby powder to laundry detergent. The chemist dilutes his drug with an inert powder, and then packages a pure product, with a standard dosage, in plastic bags with a distinctive lightning flash label. The stuff is wildly popular, since addicts know they can get a good high without being poisoned. The chemist's distributors are similarly upbeat about the product, which arrives packaged and ready to sell and which relieves them of the dangerous chore of "stepping on" the drugs. (To increase profits, street dealers adulterate, or "step on," drugs with any cheap powder they can get their hands on.)

The chemist lives in a luxurious home, and regularly entertains at tasteful dinners presided over by his fashionable girlfriend. They travel together frequently to resorts and spas. On business, of course, he travels by himself. The chemist has built his enterprise with care. He manufactures his drugs alone and forgoes opportunities to expand in order to avoid the risk of assistants. He moves his lab equipment frequently among warehouses leased under fictitious names and paid for in cash. For business he switches from his personal cars to an ever-changing variety of beaters purchased for cash, then legally insured and tagged. He has never been stopped by police while driving and has never received a traffic ticket.

He has several distributors, none of whom know each other. The chemist never personally delivers drugs or receives money. All sales and payments occur through prearranged drops and electronic transfers to banks. He rarely uses telephones, and never uses mail or computers for business. On the occasions when he meets personally with distributors, he does so one on one, without witnesses, in steam rooms, hot tubs, or on the beach, where bugs, wires, and parabolic microphones are less effective. Outdoors he invariably wears sunglasses and wide-brimmed hats so that he cannot be reliably identified from photographs or surveillance tapes.

None of his distributors knows his identity or where he lives. His minimal financial records are maintained by an accountant and an attorney in a foreign country in the name of several shell corporations. His reported income, which appears in the form of dividends from securities and equities held in offshore accounts, is ample to support his lifestyle. Taxes are paid punctiliously. His girlfriend has no idea he is a criminal; she thinks their lifestyle is funded by investments.

On one occasion police became aware of his operation. After a tip-off from a warehouse manager, they obtained a search warrant and raided his lab. The police were unlucky in their timing. They discovered only the precursors of his drug, all of which, like ammonia, are legal chemicals. Traces of methamphetamine discovered on the meticulously washed glassware proved, after analysis, too minute to support criminal charges. There were no labels or packaging materials discovered, no fingerprints anywhere in the warehouse, and no particles of skin or hair to yield DNA. Police theorize that the chemist used latex gloves, even to open doors, and disposable "clean room" suits, caps, and booties to avoid leaving biological traces.

When questioned, the chemist stood mute and police were not able to make an arrest. Subsequently he sold his house and left his girlfriend, and is thought to have assumed a new identity and resumed operations in another city. When police obtained court orders to investigate his known income, they quickly became lost in a maze of corporations in the Bahamas, the Cayman Islands, and Panama. When they investigated his driver's license, they discovered it had been obtained with a phony birth certificate.

## **THE MORALS OF THIS STORY**

1. This subject is a police nightmare: a savvy white man who works alone and does not discuss business with his women or friends.
2. Because of his general unobtrusiveness and care to drive nondescript, legal vehicles, he is almost immune from arrest by routine policing and traffic stops. Even for police detectives, this guy is a tough nut.
3. Investigating his financial affairs would require the active assistance of the U.S. Departments of State, Treasury, and Justice to enforce treaty obligations with foreign governments. For police departments, obtaining such cooperation is difficult.
4. He could be investigated by the FBI or the Drug Enforcement Administration (DEA), which have more resources than local police, but a successful prosecution would require an enormous investment of agents and

resources to keep up with the chemist's frequent moves, changes of identity, and wary business practices that negate the government's most powerful investigative tools: consensual monitors, wiretaps, and confidential informants.

### **Lets talk about attitude**

Attitude can turn a routine inquiry into an opportunity to make an arrest. Police to use "inciters" to make you flee, strike an officer, or resist. When you're upset, you're vulnerable because your emotions are raging and you can't think clearly. Cops will take advantage of this, intensify routine questioning, and then search you and your vehicle. They may use inciters, such as whispered insults or a quick poke with the baton. If they're successful in provoking you, they can upgrade a simple inquiry, traffic ticket, or misdemeanor into a felony bust. This scores more points for the cops. For you it doubles your legal fees, sends your bail amount soaring, and guarantees a stretch in the pen. It also puts a serious crime header on your NCIC information, so you can count on a lifetime of tough police scrutiny.

Assuming no serious crime has been committed, attitude determines whether you get busted. If you have committed a crime, attitude determines how you're charged and whether and how long you'll be in jail. Police have wide discretion. They can choose to set you free, give you a notice to appear, which sends you to court without being arrested, or take you downtown and toss you into the calaboose. Staying calm and polite in the presence of police is incredibly important, even if you're guilty and have been caught in the act. Attitude with cops increases the number of charges, upgrades charges from misdemeanor to felony, and allows add-on charges.

When attitude leads you to resist, it justifies police *beating the living daylight out of you!* Know what kind of medical care is available at most jails? Lousy. This means that, in the presence of police, you have to act, briefly, like middle-class Americans. Cops themselves are middle class. They respect the middle class and will cut some slack for people who act middle class. If you're poor, uneducated, and have bad manners, you're going to have to tone it *up* and act middle class for at least a few minutes. If you're rich, arrogant, and condescending, you're gonna have to tone it *down* and get humble and polite. Contrary to common opinion, cops absolutely love to bust rich guys.

### **Cops incite people into making a mistake**

#### **THE IN-YOUR-FACE SCREAM-OUT.**

This is the most common, and *legal*, inciter. During a scream-out, a cop will get an inch or so from your face and start yelling. You'll get covered with spit; your glasses will fog with hot, humid cop breath, and your nostrils will fill with whatever the cop last ate. (Pray it was doughnuts and not pizza with anchovies.) If you raise your hands to cover your face, you're "resisting arrest." If you run, you're "fleeing arrest." If you shove the cop backward, you're committing "battery on a law enforcement officer." Any of these escalates a simple encounter or penny-ante misdemeanor into a felony—more points for the cop, and more grief, expense, and jail time for you. My coauthor was actually the victim of a scream-out in the cop infested town of Miami Springs in 2000. He's a fat, balding white guy who was wearing a white shirt and tie at the time. The guy looks like an accountant or a supermarket manager. This is to emphasize that no one is immune from police harassment. There's only one arrest-proofing move when you're on the receiving end of a scream-out. This is a standing defensive position. Here's what you do.

Stand straight. Grip your hands to your pants legs. Do not put your hands into your pockets, as this can be interpreted as an attempt to reach for a weapon. Do not raise your arms, as this is considered resisting arrest in many states. Close your eyes and mouth to minimize spit ingestion. Be absolutely silent. Don't react. Don't let the cop know he's getting to you. Hang in there until the cop runs out of breath and stops yelling.

**THE TOUCHY-FEELY.** Cops will touch you, often with a hand placed softly on the shoulder, to check your levels of stress and nervousness. They may bore in with the finger or give you a shove to incite you to do something that makes you arrestable. When they search you, they may poke you in the balls or give you a hard squeeze for the same reason. This inciter is unethical, but difficult to use as a legal defense because it's done surreptitiously and is difficult to prove. You will probably be up against a wall or leaning on the cruiser while you're being searched. No matter what, stay still and do not respond to this inciter. If the squeeze hurts unbearably, *do not run or resist*. Drop to the ground in the fetal ball position. Protect your head. Try to get your head under the cruiser away from batons and steel-capped shoes. Remember, if cops start beating you, they *have* to charge you with resisting arrest. If they don't, they will be admitting to brutality.

**PROVOCATIVE WHISPERS, LEWD COMMENTS, RACIAL SLURS, ETHNIC INSULTS, AND VERBAL JABS.** When cops use racial and ethnic insults, it's illegal, but difficult to prove. An adroit cop can give you a verbal shot so quietly and unobtrusively that it cannot be heard or seen by bystanders. Many clueless people are hot tempered. Cops take advantage to whisper an insult to get you to act out and commit a felony. There are only two defenses. First and foremost, just stand there motionless and silent. Pocket the insult. Just take it. The only way you win an encounter with police is by staying free. If your brain is operational and the encounter is being video recorded (check for a small camera on the dash of the cruiser) a second defense is to position yourself so that the cop stands full face or in profile to the camera and any witnesses. This means the camera and witnesses will record his lips moving, and either discourage insults or give you a stout defense if arrested.

**THE BATON AND FLASHLIGHT POKE.** In hand-to-hand combat, police are trained to thrust batons and steel flashlights straight ahead rather than rear back and hit with them. The reason is that these weapons are more difficult to parry when pushed straight into a vulnerable body part, usually the solar plexus beneath the sternum in the center of the rib cage. They may use this training to give you a discreet poke that will not be visible to witnesses and video cameras. A shot to the solar plexus will double you over and cause you to gasp, choke, move your arms involuntarily, or throw up. A shot to the balls or throat will be even more dramatic. The only defense is to drop to the ground in a fetal ball position. This will protect you from resisting and battery charges if witnesses and cameras are present, and it will protect your body even if they aren't. This is an illegal inciter, but it is difficult to prove. Try to get your head under the cruiser. You can take quite a few shots to the ribs, but if the cops crack your coconut, you're done.

**THROW-DOWN GUNS AND DOPE.** Crooked cops can plant guns and dope on you to make a felony bust or to justify having beaten or shot you. This is a high-risk crime for the cops. If a partner squeals, or if the crime-scene guys see something odd about the setup and call for an internal affairs investigation, the cop faces indictment, dismissal from the force, and a long stretch in the penitentiary. If you survive, you can sue the city. Some courts may set aside sovereign immunity and pain-and-suffering damage caps in cases so heinous. You may end up with a pot of money, but you will do some time in jail and the hospital before you get it. When you are being provoked with inciters, practice the golden rule: **GIVE COPS YOUR NAME AND BASIC INFO, THEN SHUT THE FUCK UP!** Of course, some grunts, screams, and a bit of whimpering may be unavoidable. Those flashlights and batons really hurt. If you have to cry, just let those tears flow. I cry, too, when I go to the hospital and the morgue and see what dirty cops have done to my clients.

## “YOUR PAPERS, PLEASE”: THE CITIZEN INSPECTION SYSTEM

The primary purpose of driver’s licenses, vehicle registrations, and license plates is not to help you drive safely, but to allow the government to check on you and collect fees and fines. How can standing in line in a government office each year in order to get a sticker for your license plate have anything to do with how you drive? It has everything to do with the government having an opportunity to check where you live and whether you have outstanding traffic tickets or warrants. A huge proportion of traffic tickets are for the infraction of “failure to complete government paperwork and pay government fees.” All this paperwork ensnarls the clueless in never-ending complexities since they lack organization, reading skills, a sense of time and urgency and a permanent address at which to receive government notices. Minor traffic violations quickly escalate. Fail to pay traffic tickets and your license is suspended. Get stopped with a suspended license and you get arrested or receive a notice to appear in court.

Don’t even *think* about driving outlaw with a suspended license, unpaid traffic tickets, and no insurance. It’s not happening in the age of police cruiser computers. Cops run vehicle license tags all day, every day. When they find your paperwork out of order, it’s cop time, with vehicle search, vehicle seizure, and maybe a trip to jail. To keep that car insurance paid, settle those outstanding traffic tickets, and get your suspended license reinstated, *do whatever it takes*. Cops in need of writing a few tickets and making some cheap busts sometimes hang around motor vehicle bureau offices to catch people with suspended licenses. Cops can bust you anytime before you pay up and get your license cleared. So when you get the cash to clear your license, park your car *across the street* from the motor vehicle bureau office and stay away from cops until your paperwork is squeaky clean. Once it is, keep the paperwork in your car. Don’t assume that cop computers are 100 percent accurate and have instantly updated information. The lesson here? To avoid cops and stay free you’ve got to drive street legal. This means you must do the following.

1. Make sure your driver’s license is current—not expired, not suspended, and not, for God’s sake, revoked.
2. Make sure all traffic fines are paid, including parking tickets.
3. Keep your insurance paid up and current.
4. Keep onboard copies of prescriptions for pills you may be carrying and for insulin and syringes if you’re diabetic. Cops do *not* like to find syringes without a prescription.
5. Keep receipts for all this stuff in the car where you can reach them quickly.
6. Make sure you have no smoking tailpipes, broken taillights, or other gimmies that make you cop bait.
7. Wear your seat belt. In many states, not wearing one gives cops an easy reason to stop and search you.
8. If you carry a firearm, make sure you are carrying it legally. Each state has different laws concerning firearms.
9. You’ve got to drive safely and slowly, even if this makes you crazy.

Do you know if your license is suspended and you’re driving outlaw? If you’ve been moving around, “staying at” different places, or if you’re sloppy about reading your mail, you may not know. You don’t want to be cop bait, so find out. Here’s how. In some states, you can check your license status through the Internet or over the telephone. If this isn’t possible, you can generally go to an automobile insurance agency. They can go online with their computers and find out if your license is valid or suspended. Auto tag agencies also can do this, as well as motor vehicle bureau offices. Remember, the people you’re talking to are clerks, not cops. They can’t arrest you, so ask for their help.

**Here are some behaviors that stimulate cops to stop you when you have not committed a traffic violation.**

**THE HEAD BOBBLE AND GOOSENECK STRETCH.** When you suddenly start bobbing your head and stretching your neck to watch the cops in the rearview mirror, police may stop you to find out why you’re so nervous. When you need to sneak a peek at the cops, flick your eyes up toward the mirror without turning your

head. This will avoid the head bobble that stimulates police to stop you.

**REACHING.** Any unusual motion inside the vehicle by driver or occupant will cause police attention. Cops will presume you are hiding contraband or acquiring a weapon.

**HITTING THE BRAKES.** If you suddenly hit the brakes, cops in front of you will see your front end dip, a tip-off that you were speeding. If you're truly unfortunate, or just plain stupid, and slam on the brakes while police are *behind* you, the cruiser will crash into your vehicle. Once cops disentangle themselves from deployed airbags and bent metal, they may emerge somewhat less cheerful than before.

**PERFECT DRIVING.** Nobody drives perfectly. When cops see anyone driving perfectly, they get curious. They may stop you just to see what's up.

**DOPE FLYING OUT WINDOWS.** Clueless people think that if they toss the bags, the cops cannot arrest them for possession. Wrong. If niggers only attached their rock to a helium birthday balloon they could let their small rocks of crack go up, up and away in seconds.

**CREW CAB.** When cops see four young males in a car, they immediately wonder if this is a crew of criminals out to do a job. They also know that with four guys in a car, they are four times more likely to discover outstanding warrants, dope, guns, or stolen property.

**LOAD TILT.** When cops see a car heavily loaded and low on its springs, or tilted backward from something heavy in the trunk, they want to stop the car and have a look. Perhaps there's a dead body in there?

**DARK-TINTED WINDOWS.** When cops can't see inside a car, they like to stop the vehicle and have a look.

**DRIVER SLOUCH.** People slouching in seats appear to be *hiding from cops*. Since hide-and-seek is what police work is, cops always like to check anybody who appears to be hiding. By the way, cops like to see your hands on the wheel. They like this a lot.

**OVERLY SCRUPULOUS USE OF TURN SIGNALS.** See "Perfect driving."

**BRAKE SQUEALS.** Many brake linings have metal studs embedded in them that squeal when the brake pads wear to the point of needing replacement. When police hear these squeals, they will pull you over for an extra-thorough equipment check, with document perusal and contraband search tossed in at no charge. At the first brake squeak, run, don't walk, to get those pads replaced.

**INAPPROPRIATE VEHICLES.** Police are extraordinarily attuned to incongruities, and one of those that most attracts their attention is drivers whose visible status is different from that of the cars they're operating. If you're dirty and wearing scruffy clothes while driving a Mercedes Benz, expect police attention.

**DRIVING TOO SLOW.** Because drunks often drive very slowly, cops will pull a slow-moving vehicle in a heartbeat.

**Misc.** Wild paint jobs, Confederate flag plates, football team flags, bumper stickers, nation-of-origin flags, fuzzy dice, CDs, baby shoes, stuffed Garfields on sucker feet, "baby on board" signs, plastic Jesus statuettes, custom rims and pipes, fog lights, rear bumper propellers, and undercarriage neon lights all make you stand out in traffic. By removing these vehicle identifiers, you can hide in plain sight by blending in.

Until recently, police had to radio in to run a license plate and wait on the air while a dispatcher checked the computer and read back the information. This meant that police ran plates sparingly so as not to overload dispatchers and tie up police radio frequencies with low-priority traffic work. The installation in police cruisers of dashboard computers with high-speed wireless connections now makes running license plates a snap. Expect police to slide in behind you more frequently as they randomly check license plate numbers. Most garages and tool sheds in America have a can of the famous gray goop used to fill dents. Shade-tree mechanics slap on the Bondo but never seem to get around to finishing the paint job. Cops figure that any car with unpainted Bondo probably has equipment violations and is therefore worthy of a stop. Dope dealers often buy Bondo-covered jalopies cheap.

Once you're stopped, the cruiser will pull in behind you. If there's room, the officers will "porpoise" the cruiser in at an angle to protect themselves from being hit by oncoming traffic. The officers will approach at an angle and shield themselves at the A-post, the frame that separates the front and rear windows. If the driver or passengers draw weapons, the A-post forces them to make an awkward, three-quarter turn and spoils their aim.

**CAR APPEARANCE.** Bad guys use jalopies more than vehicles with showroom shine. If your ride is dented, rusty, and plastered with Bondo, you're on the arrest radar. Keep the car as clean as possible.

**MANNERS.** Bad guys are rarely respectful. So be polite. When talking with police, get rid of the gum and chewing tobacco to show respect. Do this with your fingers. Do not spit anything out the window or spit at the officers. Because of AIDS, spitting on a police officer is a felony in most states. Make eye contact, straighten up, and be polite, even if this makes you crazy. Turn off that stereo. Being a little nervous around cops is normal. Of course, if you're too smooth, officers may assume you're a psychopath with no emotions or that you achieved that flat affect with tranquilizers.

**DRESS.** Police rarely search cars whose drivers are wearing well-pressed suits or nice dresses. Thug clothes make you look like a felon-in-waiting. If you're nasty, scruffy, and have bad BO, expect more police attention. Not many people get searched if they have the Bible, the Koran, the Torah, or the Book of Mormon on their front seat. Liquor in a closed container is legal, but liquor in an open container is not. Some definitions are in order. "Closed container" does not refer to a booze bottle with the cork shoved back in or the cap screwed back on after you've had a few swigs. It means that the bottle was never opened and, specifically, that the tax seals, the paper seals over the top of the bottle, are intact. If you live in a city where dirty cop tricks are practiced, you should lock all liquor bottles in the trunk so cops cannot pop the seals and charge you with an open-container violation.

## **THE FAMOUS TRICK QUESTIONS**

The cops have already practiced asking these questions many times. You need to practice your responses now. There won't be time when the blue lights are in the rearview mirror. Cops always ask the questions in a casual, offhand manner, in a conversational tone. They go like this.

**COP:** "By the way, you don't happen to have any guns or narcotics in the car, do you?"

**DRIVER:** "Who, me? Uh, hmm, uh, why, no!"

1. If you say yes, you have just confessed to a crime. You have also given the police probable cause to search the car, find the illegal stuff, and arrest you. Not a great choice.

2. If you answer no and a subsequent search or inventory discovers dope, unregistered guns, bongos, or stolen property, you're toast. Regardless of your answer to question 1, cops will immediately take their money shot and ask question 2.

**COP:** “Then you won’t mind if I make a search, will you?”

**DRIVER:** “Uh, well, er, hmmm, uh, why, no!”

Decline nicely with just the right amount of citizen indignation. You must rehearse this in advance, however. Without practice you will never get this right when cops are standing in your window shining flashlights in your eyes. It goes like this: “*Officers, I apologize for the traffic violation. I have answered your questions and cooperated with you in every way. However, I am late and urgently have to be going. \_\_\_\_\_ (Fill in the blank with a truthful reason). Are we finished? May I go now?*” You fill in the blank with the reason you have to go. This must be plausible and, preferably, truthful. It must realistically fit in with your personal circumstances. Remember, many things you say can be *verified* by police.

For example, if you say, “I need to get home to take care of my mother, who’s sick,” the cops may call your mother on their cell phones to check. The following are some typical reasons cops should let you go on your way. I’m diabetic (asthmatic, have heart disease, etc.), and I have to get home to take my medicine. I need to go to the bathroom. If I don’t go soon, I’m going to pee in (or crap) my pants. You can just say that you *do* mind. Once you say no, the police cannot search your car without a warrant or probable cause.

## **WHAT HAPPENS WHEN YOU SAY NO?**

When you say that you *do* mind, this puts the cops in a quandary. They will do one of the following.

### **1. SEARCH FOR PROBABLE CAUSE.**

Cops may call on the radio for a K-9 unit. When the dog arrives with its handler, it will sniff around your vehicle. If it “alerts,” usually by scratching the vehicle, the cops have probable cause and can search your vehicle without a warrant and without your permission. When they find the stash, you, of course, are in the doghouse. Cops may also call a supervisor to discuss whether they have probable cause. Both calls, to the supervisor or to a K-9 unit, require that the cops stay out of service by the side of the road. As long as the cops remain on the side of the road, they are out of service and can’t respond to calls. They are at risk of committing a serious cop screwup called annoying the sergeant. However, if you have a high A-Q, i.e., you look like a suspicious, high-value target, cops will wait it out to get a clean bust. The sarge may even join them to get in on the fun.

### **2. Cops can try to get a warrant from a judge or magistrate.**

This isn’t easy at night or on weekends. Many jurisdictions do not have magistrates or judges who are available outside business hours or who will issue a warrant requested by telephone. Cops may release you rather than go through the hassle.

### **3. Cops may arrest you by using either of the following methods.**

If they don’t have a solid reason to arrest you, they may use inciters to get you to do something clueless, like fleeing or trying to hit them. They may fake their way to an arrest and probable cause for a search. In the arrest report they may write something like “subject appeared suspicious” or “subject smelled of marijuana.” As probable cause, this is weak. A good attorney often can get charges dropped or substantially reduced when this occurs. Unfortunately, even a bad arrest gets you processed into the electronic plantation and ruined for life.

### **4. Cops will try to use the “inventory” scam to search your towed car.**

Post arrest, cops can impound the car, call for a tow truck, and conduct an inventory so you cannot claim later that the car contained money or valuables that were stolen. There’s not a lot of difference between an inventory and a search. If you’re carrying dope, guns, dead bodies, or stolen merchandise, they will be found. If your car is trashed during the inventory, the amount you can recover from the city is strictly limited by statute in most states and usually does not cover actual damages.

You should always refuse a search *when the car is dirty, you're guilty as heck, and you know it*. Refusing the search will preserve your defenses. You'll need them. You're going to be arrested, so now the aim is to reduce the damage. The more work the cops do to search your vehicle, the more likely they are to make mistakes that can result in charges being reduced or dismissed. You might get lucky. If cops make a perfunctory search, they might not find anything. The cops might get an urgent radio call and set you free in order to respond. The K-9 could be tired. Most people don't know that police dogs can only scent drugs reliably for a few hours a day. After that their sniffers conk out and they can miss the dope.

### **WHAT TO DO DURING A SEARCH**

When your car is being searched by police, whether by your consent or due to probable cause, you should do the following:

1. Ask permission to sit down. Sitting will prevent your following behind the cops and "alerting" with your body language when they get near the contraband. Cops FREQUENTLY have an officer watch your facial expressions as they search your car or house. Sitting down will also help you avoid confessing, babbling, or lying. It will minimize cops' ability to judge your body language and smell your breath for booze or drugs. Always ask permission first. If you sit without permission, police may consider this to be fleeing or resisting.
2. Face away from the police and the vehicle. This will help you cool down and reduce your ability to "alert."
3. Shut the fuck up! Do not speak. Do not utter any sound whatsoever. Any noises you make or words you say are evidence against you. Once cops begin the search, nothing you say will cut it short. If you keep talking to distract police, they will only intensify the search.

### **WHAT TO DO WHEN YOU'RE ABOUT TO GET ARRESTED**

- 1 Ask for a notice to appear, or penal citation, especially if the problem is small amounts of drugs or something else that's relatively minor.
- 2 Cry and beg not to be arrested.
- 3 As a last-ditch technique, vomit on yourself and shit your pants before the officer decides to arrest you.

**Thank you for reading our eighth edition**

**Visit [Resist.com](http://Resist.com) to buy future and archived editions.**

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the "\_" character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**

# The PARANOID Newsletter

Because they ARE out to get you.

A good walker leaves no tracks;  
A good speaker makes no slips;  
A good reckoner needs no tally.  
A good door needs no lock,  
Yet no one can open it.  
This is called "following the light."  
*-Tao Te Ching*

## Introduction

This is the ninth issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding fathers say if they were alive today!

**Destructive entry** (or forced entry) is a non-covert method of entry characterized by damage to or destruction of a lock, safe, or surrounding objects, such as a door, window, or wall. It is by far the most common method of entry and is frequently used by law enforcement and military personnel for rapid entry to a residence or facility. As you might have guessed, there are many ways to destroy things. Techniques are classified by their method of destruction in terms of the physics of the operation but often overlap and complement one another. All destructive techniques use energy or force to damage, displace, weaken, or destroy components. Once components of a lock, safe, door, window, or wall lose structural or molecular integrity their ability to resist compromise is considerably reduced. The general categories of destructive entry are: chemicals, compression, impact, shearing, temperature, tension, and torsion.

While the techniques discussed might seem advanced, the majority are rather simple when put in perspective; doors are kicked in, padlock shackles are cut, locks are drilled, et cetera. Techniques are categorized to help the investigator identify, define, and study new attacks. While tool designs differ greatly the tool marks and forensic evidence they leave behind may help investigators quickly identify the techniques used to gain entry.

## Destructive Entry Principles

**Chemicals** are used to affect the molecular structure of components. Chemicals, namely acids, can corrode, disintegrate, or dissolve components. Like temperature, chemicals often leave components vulnerable to other attacks.

**Compression** is the use of pressure against a component in complementary directions. Essentially, the opposite of tension. It causes distortion, compaction, or breakage of components. Compression is most often used to reduce the strength of materials so that other methods can be used.

**Impact** is the use of pressure and shock against a component. Striking and explosives are most common. Impact has a wide variety of results including fracturing, breakage, deformation, and compression. Some methods of bypass use impact to retract the locking bolt, most of which are destructive. Explosives are one of the most dangerous methods of destructive entry and use has dwindled with time as safer alternatives, such as drilling, have

become popular.

**Shearing** is the use of pressure on a component placed between two edges. Cutting, chopping, and drilling are included in this category. Drilling is the most popular method of destructive safecracking and removal of locks by a locksmith. In general, drilling is probably the easiest, fastest method of destructive entry.

**Extreme temperature** can be used to affect the molecular structure of components. High temperatures can vaporize, burn, melt, or re-temper components. Re-tempering can leave components soft or brittle, thus vulnerable to many other attacks. Low temperatures are less common, but can be used for similar purposes.

**Tension** is the use of pressure on a component in opposite directions. Stretching, pulling, prying, bending, or ripping are included in this category.

**Torsion** is the use of rotational pressure (torque) on a component. Twisting and torque are included in this category. Causes shearing, compression, and deformation of components.

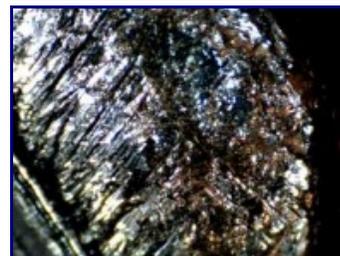
Destructive entry is fairly straightforward in terms of method of entry, so the focus is on tool mark identification. The forensic locksmith must be wary of destructive techniques used as a method of hiding covert or surreptitious entry. A thorough investigation will reveal covert techniques and can potentially rule out destructive entry as the method of entry due to improbable direction, angle, or position of tool marks.

### Forensic Evidence

The most common attack against padlocks is cutting the shackle, either in half or clean off. Almost all low to medium security non-shrouded padlocks are susceptible to this attack. This attack is a form of shearing, and the two edges of the bolt cutter are clearly seen in the displacement of the shackle material.



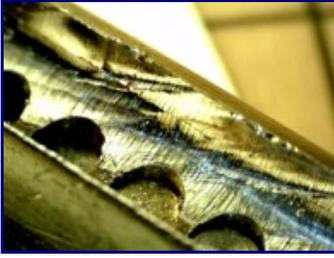
A closer examination of the tool mark reveals that a red substance is present in the area where the bolt cutter was used. This could be a variety of things; paint, dirt, grease, or rust. We might be able to match this material to the tool if a bolt cutter is found in a suspect's possessions.



Drilling, a form of shearing, is the most common method of destructive entry against all types of locks. It is frequently used by locksmiths to remove locks when they cannot be opened non-destructively. In this photo, the plug of a KIK cylinder has been drilled at the shear line, allowing the plug to freely rotate.



On the Forensic Investigation page we discuss the need to tape any openings in locks recovered at the crime scene. In the photo, a large amount of metal is present inside the lock, a product of drilling. This material is preserved because it may contain evidence useful to the investigation, such as shards of a broken drill bit.



Drills are much like firearms in terms of forensic evidence. Bullets fired from a gun have striae based on the barrel used; the same goes for drill bits used in destructive entry. In the photo, the spiral striae left by the drill bit can clearly be seen in the plug of the lock.

Impact is a versatile method of destructive entry that is extremely effective against windows, doors, and walls. In the photo, a padlock has been hammered until the shackle broke. The direction of the break can tell us what angle it was being struck from. Additional tool marks will likely be found on the body of the padlock.



In this photo, the body of the padlock shows tool marks in places where the hammer impacted the lock. The crescent shaped marks are numerous and can be measured to determine the size and shape of the hammer used. At least three different points of impact are visible.



Heavy damage to the face or keyway of the lock can mean many things. A thorough investigation of tool marks, including angles and positions, helps to reveal how entry was accomplished. In this photo the keyway has been considerably widened and gouged so a tool can be inserted, probably a screwdriver or chisel.



In addition to damage to the keyway, the upper pin chambers have been completely sheared off, leaving the plug and broken cylinder free to rotate in the lock. This attack appears to be torsion applied counter-clockwise to the plug through the use of a screwdriver.

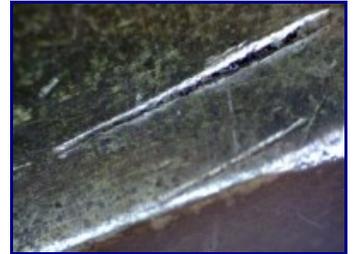


The pins inside this lock show heavy damage from where the screwdriver or chisel was forced into the keyway. Examination of what is left of the tip of the pin shows no indication of covert entry techniques. Because of the force used, tool marks on the pins are rather distinct and may later be used to link suspects to the crime.

European profile cylinders are held in place by a screw that extends through the center of the cylinder. Because the cam is beneath this point, it is the thinnest part of the lock and thus the easiest to break. In this photo, a european profile cylinder has been snapped in half (forced to the left) using common hand tools.



The basis of this attack is that there is enough of the cylinder extending through the door, as little as a few millimeters, and a tool used to grab and apply force to the lock. In this photo, tool marks can be seen where the tool was used to grab the front of the lock.



The cam of the lock can also be examined to determine which way the lock was snapped. This is generally not important, but the lock may have been snapped at an angle that is impossible when the door is closed, indicating fraud or misdirection from the real method of entry.



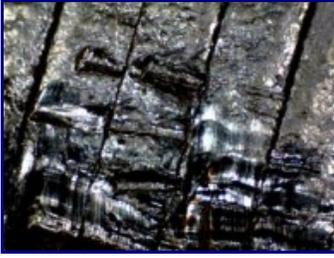
Many destructive attacks against low security padlocks break the shackle because, relative to the body, it is the weakest component. In this photo, the padlock shackle is broken in two places, with one piece being stuck beneath the locking bolt.



A thorough examination of both the shackle and the padlock body helps to identify the specific technique used. In this photo, the body of the padlock shows excessive distortion in the form of twisting, indicative of extreme torsion being applied to the padlock body.

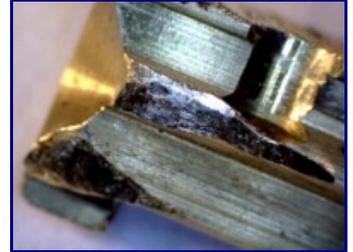


Tool marks for the torsion tool are found on the edges of the padlock. Marks appear to be rather fresh, thus the most likely candidates for the attack in question.



A closer inspection of the tool mark shows a series of parallel teeth marks, probably from the use of a plumber's wrench or tongue-and-groove pliers. Marks can be used in tool mark comparisons done with tools found in a suspect's possessions.

Simulating lockpicking is common in insurance fraud or when the insurance holder is worried about coverage. These people rarely understand lockpicking and just jam a screwdriver in the lock to make marks. In most cases, material removal and tool marks are present at the front of the cylinder but not past the first or second pin.



The pins in simulated lockpicking will have a large amount of material removal and tool marks that are not consistent with any type of covert entry, including lockpicking or key bumping. Marks will usually not be found on the pins in the back of the lock, too.



Chemicals are powerful because they can fundamentally alter metals to leave them vulnerable to many other attacks. In this case, brass pins are dark red/brown because of  $\text{NO}_2$  fumes released when concentrated nitric acid contacted the brass components. Nitric acid has the effect of eating away the copper in brass.



A closer examination can confirm the use of nitric acid by identifying trace evidence left by the chemical reaction between nitric acid and brass. The scattered blue particles are cupric nitrate and zinc nitrate, a byproduct of the chemical reaction.

### **Forensic examination of lockpick toolmarks**

In almost all cases of lockpicking two tools are used. A tension tool is used to gently apply tension to the lock, and a pick is used to position components. As tension is applied to the plug, bolt, or other component, locking components will bind in some way. The pick can be used to determine which component is binding and then used to position it properly. The correct position of a component is known by the attacker through feedback in the form of touch, sound, or sight. The tension tool holds properly positioned components in place, and the attacker repeats the process. Once all components are properly positioned the lock can be unlocked or locked.

The nature of lockpicking necessitates that strong materials be used for tension and picking tools. Tools are commonly made out of steel, iron, and aluminum. Tools are thin (on average 0.025 with pin-tumbler picks) and

require a medium amount of force to move locking components. When contacting the softer brass or nickel-silver of locking components, pick and tension tools leave marks in the form of gouges and scratches. The best source of forensic evidence of lockpicking are on the components themselves, but the lock housing, bolt, and cam may also be examined, depending on the type of lock.

### Forensic Evidence

The act of using a pick tool is invasive, and we expect the stronger material of the pick tool to cause marks on the softer brass or nickel-silver of the lock components. In this photo, we see scratches where the pick tool was used to lift the pin. These appear to be single-pin picking marks due to their shape and consistency.

This photo is similar to the last, but instead there are many varied, elongated scratches at different angles and depths on the pin. This type of marking is indicative of a pick that is designed to be gently rubbed against the pins at varying height and tension. Of course, this is the technique known as raking or rake picking.

In this photo, marks left appear to be a combination of both picking techniques. Many attackers will attempt to lightly rake as many pins as possible and then proceed to use single-pin picking against the rest. This may be necessary in the case of security pins that are triggered while raking, also.

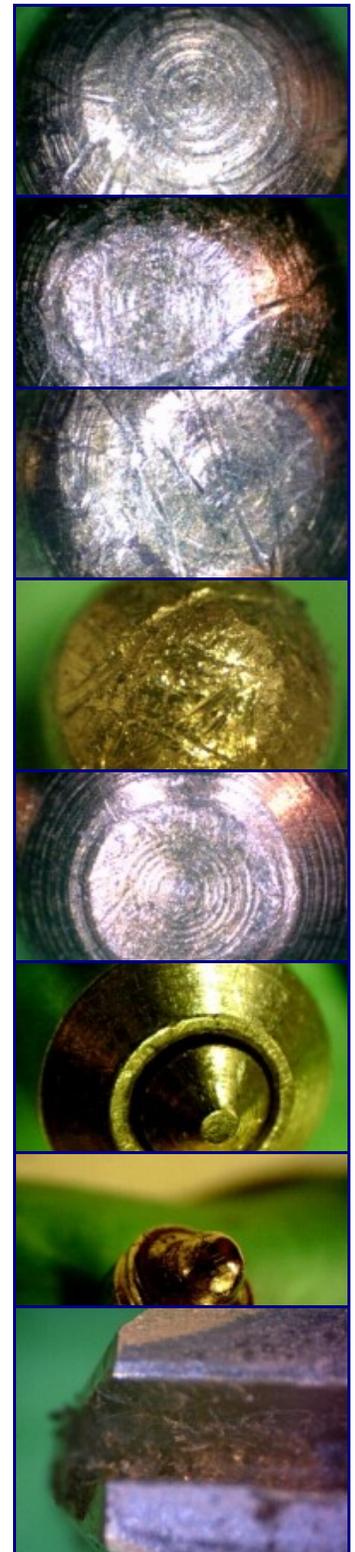
The marks left by an attacker are in many ways indicative of their skill level. In this photo, extremely deep and plentiful pick marks are shown. The attacker, an amateur, used extreme force on both tension and pick tools. The extreme tension causes pins to bind against plug and require more force to be lifted.

This is a very skilled attacker who uses extremely light tension and picking force to reduce forensic evidence. Despite skill, we still find similar forensic evidence. In this photo, pick marks are extremely light but still visible in the center of the pin. We can also see some marks on the side of the pin which are more defined.

There are many other designs of pin-tumbler besides the standard round or pointed tips. This is a photo of a Mul-T-Lock telescoping pin tumbler that uses an inner and outer pin stack. Both show signs of picking tools. If we separate the pins, we would also probably find picking marks on the inside chamber of the outer pin.

Some pin tumbler designs are rather strange, designed to deter manipulation. This photo shows a Vachette VIP "nippled" pin. The design of this pin is rather complex, with not only a nippled tip but also a very spool like appearance. In any event, picking marks are visible along the nipple and base of the pin.

Forensic evidence is also left behind by various lock-specific tools, which are growing more common with high-security locks. In this photo, the pick marks from a Medecoder type tool are visible in the sidebar channel where the tool was used to rotate the bottom pin.





For the attacker, it is difficult to not touch the sides of pins. This can happen during raking as well as single-pin picking. Marks left on the sides of pins are quite noticeable and not as prone to wear and those in the center of the pin. In the photo, light scratches at varied angles are visible.



In the case of low-high pinning combinations it is even harder to lift pins without touching the sides of other pins. In this photo, a series of long scratches travel up the side of the pin. Interestingly, we may be able to measure the length of scratches to determine if the attacker raised the adjacent pin high enough.



Like the bottoms of the pins, the sides can tell a great deal about the skill level of the attacker. In this photo, gouges on the sides of the keys are rather deep, caused by extreme force being used on both the tension and picking tools. With this much material removed, it may be possible to identify pin material on a suspect's possessions.

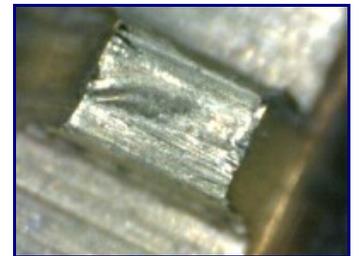
The movement of the pick through the keyway also leaves forensic evidence in several places. The most common is on the walls of the plug itself. In this photo, scratches left by the pick tool are found below the pin chambers on the walls of the plug. The scratches are at various angles inconsistent with the use of a key.



One of the best places to look in the plug is at the top of the keyway. The key will never touch this area, so it is one of the few "virgin" areas in the lock. In this photo, we can see that there are light scratches along the area before the first chamber, probably from the use of a tension tool at the top of the keyway.



Marks on the warding inside of the plug are also common. Normal use of keys does not usually cause these marks, but if they are indeed the cause marks should be present on several other wards, as well. In this photo, a deep gouge has been made by the pick tool on one of the wards deep inside the plug.



Marks may also be left in the pin chambers themselves. In this photo, we see a mark on the left side of the pin chamber. This area of the plug cannot be touched by the key and pins would not make a mark like this unless they were severely deformed. Compare with the chamber wall on the right.

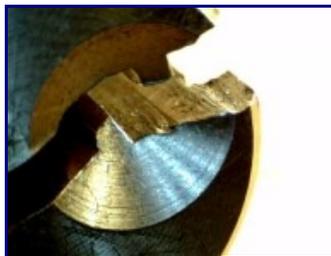


We might find pick marks higher in the pin chambers, too. These areas are subject to wear as pin stacks are moved by the normal action of the key. In this photo, an up-down-up patterned scratch is seen. This is probably caused by the attacker lifting and lowering the pin stack, trying to find the



shear-line.

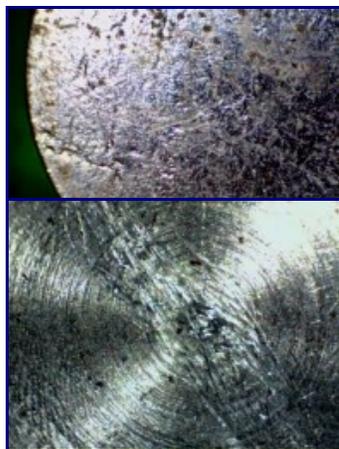
Forensic evidence of the tension tool can also be identified rather easily, especially if the attacker is a beginner or amateur lockpicker. The act of putting tension on the plug causes the tool to lightly shear the plug walls. In this photo, we can see the gouges left by the tension tool being placed at the bottom of the keyway.



Destructive disassembly of the plug lets us get a better picture of tension tool marks. In this photo, we can see that there is a deep gouge where the tension tool was actually used, as well as several scratches below it. The scratches are likely from positioning of the tool or tapping it with the picking tool while picking.



In the case of a skilled attacker, very light torque is applied to the tension tool. It may be more complicated to identify marks without proper lighting, but even in this example, where low tension was used, the tension tool marks can be identified when they are properly illuminated.

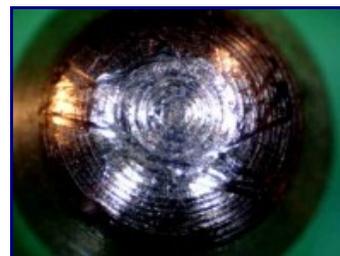


The cam may also have marks because many attackers, when navigating the back of the plug, will hit the cam. This is especially true of less controlled techniques like raking. In the photo, a light scratch is present in the center of the cam, a place the key normally does not touch.

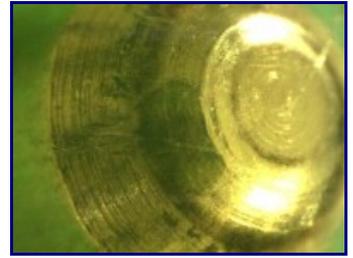
One of the problems as an amateur is knowing where the pick is. It is common to see many amateurs with the tip of the pick poking out of the cylinder. When the cam is on, this may translate into extreme scratching on the back of the cam, as seen in this photo. Similar marks may be left by some forms of bypass.

### Effects of wear

The question always arises as to how we can determine when pick marks were made or how long it takes normal wear to remove them. In this photo is the first pin from a lock that has been picked once. We will use this as a reference to see the effects of wear after 250 uses.



After 250 uses (roughly 2-4 months use) the tip of the pin has been worn by the key, leaving fewer distinct picking marks. At the same time, the sides of the pin still show very clear and distinct picking marks. This is because the key does not touch these areas as frequently and may never, depending on the key biting.



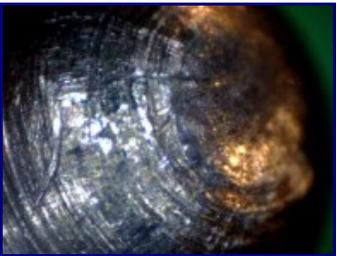
While taking the last photo I noticed a strange shape in the top right of the photo. When I refocused in that area I found this. It appears to be a small piece of brass that has transferred to the tip of the pin, probably a very small fragment of the key. Quick, call the crime lab!



### Non-metal Lockpicks



Carbon fiber lockpicks were considered for use in Anti-Forensics, but my research shows that they leave marks similar to traditional metal lockpicking tools. The photo shows a finished carbon fiber lockpick in the half-diamond design. This pick is roughly 0.025" thick.



Carbon fiber picks did not work as well as I had hoped. Most importantly they fell short of surreptitious by leaving marks on pin-tumblers similar to traditional tools. In this photo, light scratching along the tip and side of the pin can be seen, caused by a carbon fiber lockpicking tool.



Carbon fiber lockpicks also seem to grab and hold pin materials much better than their metal counterparts. In the photo, a carbon fiber pick is shown with brass residue from the pins of a lock it has picked. This can be used in court as evidence to link a suspect to a crime.

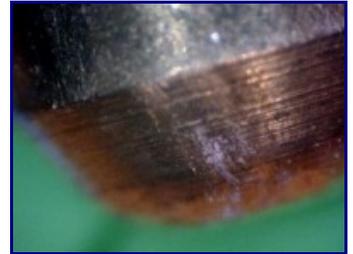
Also considered for Anti-Forensics were fiberglass based lockpicking tools. My research shows that these are also unsuitable because they leave distinct forensic evidence on the pins and inside the plug. In this photo, a half-diamond fiber glass pick is shown. This pick is roughly 0.028" thick.



Fiberglass also left various traces similar to traditional metal lockpicking tools. In this photo, parallel scratches at various angles and positions can be seen on the bottom and side of the pin-tumbler. All marks were cause by the fiberglass picking tool.



Fiberglass is also less surreptitious than carbon fiber because the act of picking and raking the lock leaves behind a sizable amount of fiberglass on the pin-tumblers and walls of the plug. In this photo, fiberglass residue can be seen on the tip of the pin-tumbler.



Like carbon fiber picks, fiberglass does a very good job of trapping trace evidence from the pin-tumbler inside the lock onto the pick. In this photo, the tip of the fiberglass pick is shown with light brass residue and lubricant (black) clearly visible.



**Thank you for reading our ninth edition**

**Visit [Resist.com](http://Resist.com) to buy future and archived editions.**

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**

# The PARANOID Newsletter

Because they ARE out to get you.

A good walker leaves no tracks;  
A good speaker makes no slips;  
A good reckoner needs no tally.  
A good door needs no lock,  
Yet no one can open it.  
This is called "following the light."  
*-Tao Te Ching*

## Introduction

This is the tenth issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding fathers say if they were alive today!

## Principles of pick gun forensics

Manual pick guns are spring-loaded tools that resemble a toy gun with a lockpick attached to the front. The lockpick is interchangeable, and referred to as the "needle." To open the lock, the needle is inserted in the lock and placed under all pin stacks. As with lockpicking, a separate tension tool is used to apply tension and rotate the plug. Light tension is applied to the tension tool and the trigger of the pick gun is fired. According to physics, the kinetic energy transfers from bottom pin to top pin, causing the top pins to "jump" in their chambers. If all top pins jump above the shear-line at the same time, the plug can be rotated to unlock the lock.

Electric and vibrational pick guns work on a similar principle, but instead oscillate the needle back and forth, causing it to vibrate. The tool is controlled to get the resonating frequency of the needle at the right point so that top pins jump above the shear-line.

The main source of forensic evidence with pick guns is on the bottom of the pins, where the needle strikes. We may also see marks in the plug if the needle is not properly positioned and makes contact with the plug walls when triggered. The cam on the back of the lock may also have marks if the needle is inserted too far into the lock. As is the case with lockpicking, we can also identify tool marks left by the tension tool.

In the case of vibrational or electric pick guns, we will see considerably more evidence on the plug walls because the device is constantly moving.

The striking of the pick gun needle against the bottom pins causes very clear forensic evidence. Unlike picking, which causes scratches, the pick gun causes impact marks that, when done many times, begin to resemble the spokes of a bicycle along the circumference of the pin.



The marks left by a pick gun are so distinct, compared to the rest of the pin, that it is often possible to count them to determine how many times the pick gun was triggered. Each time the needle strikes, the bottom pins may rotate slightly, allowing marks to be separate and distinct.

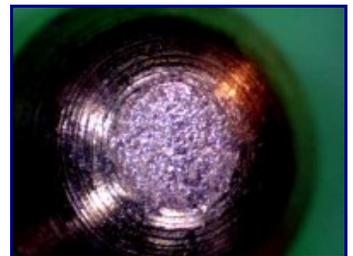


As with many other techniques, the cam of the lock is a good source of forensic evidence. This is sometimes the best evidence, because the needle of pick gun often shears very clear marks into the cam. In this case, the pick gun appears to have been used at least eight times.

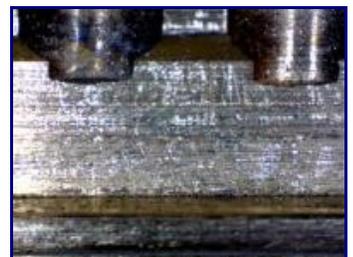


Up close we can see the very distinct markings left on the cam by the pick gun needle. These marks are well defined and would make for a very good tool mark comparison. Because they are so deep, the pick gun needle may also have material residue that can be linked back to this cam.

Electric and vibrational pick guns leave different marks because they are constantly moving in the lock. When using this type of pick gun, material removal from the components and plug is so extreme that you can see brass particles exiting the keyway. In this photo, repeated use of a vibration pick gives the bottom pins a rough, uneven texture.



Constant movement of the vibrational pick gun needle causes numerous tool marks on the plug walls, as well. In this photo, various vertical scratches are present throughout the length of the plug. Some vibration picks also leave a stuttered or angled type of tool mark on the plug walls.



### Principles of key bumping forensics

To bump a lock, a key is acquired that fits the keyway of the lock. The key is modified so that all cuts are at their lowest depths or lower. This is commonly referred to as a "999 key," because 9 is usually the designated lowest cut depth. If done by hand, a key gauge or micrometer can be used to measure the key and ensure cuts are deep enough. If done with a key machine, the key may be duplicated from a working bump key, or cut by code to the lowest depths.

In the pull-out method, the key is inserted into the lock fully then withdrawn one pin space. In the minimal movement method, the key is further modified by removing material from the tip and shoulder of the key. The minimal-movement key is inserted completely into the lock. In both cases, light tension is applied to the key and a tool (known as a bump hammer) is used to impact the bow of the key, causing the key to be forced into the lock.

The impact on the key causes kinetic energy to travel from the key to the top pins, causing the top pins to momentarily jump. If all top pins jump above the shear-line while tension is applied the plug is free to rotate.

As with pick guns, the main source of forensic evidence of bumping is on the pins themselves. The action of striking the bump key into the lock causes distinct dents and scratches on the bottom pins. Bumping also affects the face of the plug, the keyway profile, pin chambers, top pins, and the bump key itself.

### Forensic Evidence

The act of key bumping basically slams the key against the bottom pins to allow for kinetic energy to be transferred from the key to the top pins. Because they are immobile and absorb the kinetic energy, this causes considerable damage to the bottom pins in the form of large dents and scratches.



A bump key that is cut by hand, with a low speed key cutter, or made of a considerably stronger material (steel, iron, nickel-silver) than the pins may act as a file as it impacts bottom pins. In this photo, light scratches can be seen traveling through the bumping dent.



Alternate lighting may be used to illuminate bumping scratches and dents more efficiently. In this photo, there are dents on the left, center, and top of the pin, as well as scratches. In many cases it is possible to count the number of times the bump key was used by counting the dents.



Bumping is rarely 100% successful, either because bottom pins are bumped above shear line, or top pins are not bumped high enough. When this happens the tension applied will misfire, causing one or more top pins to bind. This causes light shearing against the bottom of the top pins.



Some top pin designs will be more affected by bumping than others. In this photo, a spool pin with serrated edges is shown. Repeated bumping of this pin has caused the serration to close up (compare with previous photo). In general, situations like this slightly decrease pick resistance.



In some pin designs the bottoms of the top pins will be considerably damaged by bumping. In this case, the bottom pins are lightly rounded on both sides, allowing them to be inserted either way. When bumped repeatedly, the bottoms of the top pin become considerably dented.

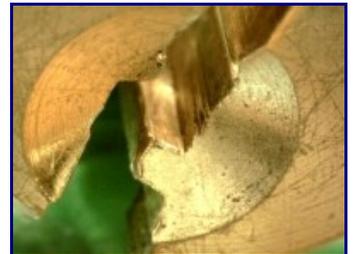
The pin chambers within the plug may also be damaged by bumping. When kinetic energy does not properly transfer to the top pin, the pin stack may instead press against the chamber walls (caused by the movement of the bump key). Repeated bumping may cause these areas to distort, stretching in various directions.



One of the most noticeable pieces of evidence from key bumping is damage to the face of the lock. This is caused by the shoulder of the key impacting the area above and below the keyway. The use of modified shoulders may prevent this from happening.



In the minimal-movement method, material is removed from the tip and shoulder. This makes the method work but also inserts the key far enough that in some cases affects the keyway. This is due to the key material getting thicker as it reaches the bow. In the photo, this can be seen around the edge of the keyway.



Many unskilled attackers may attempt to bump unbumpable locks. This will probably damage the lock and borders on breaking the lock completely. In the photo, an EVVA 3KS wafer is shown after an bumping attempt. The wafer arm has broken off and a large dent is present, this lock was non-functional after this.



In this photo we see the cylinder from the failed bumping of an EVVA 3KS. The serious damage to the walls of the cylinder is due to the wafers slamming against the cylinder when bumping was attempted.

Manipulation-based impressioning works by taking a blank key that fits a target lock, applying extreme torque to the key (thus binding components), and manipulating the key blank in order to produce marks on the key. This is correct for pin-tumbler locks, but the actual process varies for different lock designs. The theory behind impressioning is that components at the wrong position will bind and become immobile. When the soft brass key contacts the immobile components, a mark should be produced. When a component is properly positioned it should

no longer bind and thus no longer leave marks. The blank is used to gather marks, then filed in those positions. This is repeated until all components are in their proper position and the lock opens.

Because this type of manipulation is stressful on the key and cylinder we expect to find various types of forensic evidence. Namely, it is expected that the forceful binding of bottom pins, all of which are raised at or above shear line, to cause marks. We may also find material transfer from filing the key if the attacker is not careful to properly clean the key after each filing.

There are variations on the manipulation process that use pressure responsive materials, such as lead, tape, or plastic to facilitate the process of impressing. In these cases we may also find material transfer as the soft materials rub against the keyway and inside of the plug.

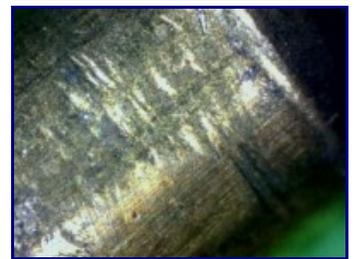
Of course, the key used in manipulation-based impressing will provide a good deal of forensic evidence.

### **Forensic Evidence**

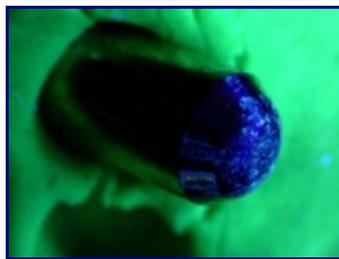
Because we are forcibly binding bottom pins at or above the shear line we expect to see marks on the pins where this occurred. In the photo we can see several marks where the pin was bound against the plug in the form of straight lines sheared into the pin. (Note: the scratches to the left are pick marks)



Sometimes, impressing marks are so clear that we can count the rounds of impressing. If marks are far apart the forensic locksmith can also measure the distance between them. This may indicate a more skilled attacker if they are using factory depth increments to speed up the impressing process.



The key blank may be specially prepared for impressing via manipulation in a variety of ways. One of the possibilities is the use of Ultraviolet ink and an ultraviolet light source. This is an interesting technique, but as you can see in the photo it leaves ultraviolet ink residue on the face and insides of the lock.



When using UV impressing, UV ink is reapplied each time the blank is filed. In turn, the pins will have a large amount of UV residue on them. Notice the obvious key pattern of UV ink across the sides of the pin. In addition, the UV pen fibers may have been stuck to the key and left behind on the pins or the plug walls.

### **Decoding Principles**

Keys can be directly examined and decoded. Key decoding focuses on identifying the pattern of biting cuts on the key. These can be determined by looking at the code numbers stamped on the key, or through direct measurement of each cut with a ruler, micrometer, or caliper. These measurements are used to determine the manufacturer's biting code so that a key may be easily made. Sophisticated locksmithing tools are available that will automatically identify the biting code based on the cuts and keyway profile of the key. This is the most basic of decoding

methods, and may be problematic with high-security keys that have advanced features like sidebars, angled biting cuts, moving parts, or magnetic/electronic components.

Components inside the lock can also be decoded through invasive, manipulative tools. These tools have radically different designs, and are generally specific to particular brand or model of lock. Most manipulative tools focus on measuring each component to determine: weight, range of movement, shape, spacing, and alignment. Many manipulative decoding tools resemble traditional lockpicking tools with the addition of a measurement device. Opening the lock via lockpicking is sometimes a pre-requisite to decoding the components. Many tools also decode the lock as they pick it. The standard tubular lockpick and the Sputnik tool are the most popular examples.

Disassembly of the lock can also be done to directly measure all internal components. This can be a complicated procedure depending on what type of lock it is and how it is installed. This process usually requires the lock be compromised first so that the door can be opened. Facilities with lax security measures may leave doors unlocked and unguarded, allowing someone to quickly remove, disassemble, and decode a lock. Reassembly and reinstallation of the lock is equally important, and if done incorrectly can cause the lock or proper key to no longer function.

**Visual/optical decoding** focuses on observation or surveillance of the key or internal components without needing to invasively manipulate them. A photograph of a standard key's biting is enough to decode the biting code. Surveillance may be used against combination locks to observe the correct combination being entered by an authorized user. Optical decoding uses tools like borescopes or otoscopes to look inside the lock at the internal components. Optics can be used to look at the size, shape, color, alignment, and spacing of internal components.

**Radiological imaging** is a form of surreptitious decoding that uses penetrating radiation (X, beta, and gamma rays) to "see" inside the lock or safe, revealing the proper positions of components. This is most often used against rotary combination locks to determine the position of each gate in the wheel pack. While very effective against many combination locks, it is expensive and only used by medium-high skill attackers.

**Thermal imaging** is another form of surreptitious decoding that uses special devices to look at thermal residue left on keypad or pushbutton combination locks. This reveals buttons recently pushed, but may not directly reveal the combination sequence. Like radiological imaging, this is generally not used by low skill attackers.

As you can see, decoding is a vast array of techniques with forensic evidence equally varied. Manipulation-based decoding tools provide forensic evidence that is similar to lockpicking, but may vary depending on the specific techniques. Examination of keys may leave forensic evidence depending on the type of tools used. Visual, optical, radiological, and thermal decoding are all considered surreptitious and leave no lock related forensic evidence.

### Forensic Evidence

Colored components are a red flag that optical decoding may be possible. The colors signify the size of components, and can be viewed with a borescope or otoscope to decode the lock. Colored pins are rare in factory-original locks, but are popular in many do-it-yourself lock repinning kits.

Low security wafer locks can be visually or optically decoded simply by looking at the size of the wafers. Unlike pin-tumbler locks, wafers block at the same position outside above the plug. Keying is made possible by varying the amount of material in the middle of the wafer, causing it to be raised high or lower by a key.

Keypad-based combination locks can often be visually decoded based on wear. In the photo, the worn down numbers help to reduce the search space to only a few combinations of numbers. It is possible that the combination is meaningful to the



owner, such as their birthday year or lucky number.

## **Anti-Forensics**

Forensics is a never ending cat and mouse game. Investigators look for better methods to determine what happened while attackers are look for better ways to cover their tracks. This section discusses so called 'anti-forensics,' various techniques and methods to conceal evidence of entry.

Entry techniques that leave no forensic evidence are known as surreptitious entry. While technically surreptitious and leave no forensic evidence, the act of using them may leave non-lock evidence. When we talk about "no forensic evidence", we mean as it relates to the examination of the lock, safe, or related components, other forensic evidence may still be available. For example, forensic evidence may be found in the form of fingerprints on a safe dial, hair, fiber, footprints, surveillance, et cetera.

In many cases the forensic locksmith is asked to provide an assessment of how plausible certain surreptitious entry techniques are against a given lock. This can be done through a series of laboratory tests, an analysis of the required skills, tools, or money required, and examination of the installation and configuration details of the lock. Cases of completely surreptitious entry are viewed by the investigators on the basis of what facts and logical conclusions present themselves.

## **Anti-Forensic Materials**

The idea of anti-forensics materials in tools is a popular but not well researched (publicly) area. Lockpicks made of soft materials such as wood or plastic would, in theory, not leave any marks on the considerably stronger brass, nickel-silver, or steel components. While they sound great in theory, they are considerably harder to use in practice. Tools made of these materials are considerably weaker, less maneuverable, and more prone to fracture or breakage than the steel normally used in tools. These types of tools also exhibit drastically reduced feedback capabilities, important in many covert entry techniques, when compared to metal. Coating standard tools with other materials has also been attempted, with limited success. The best example is teflon coated lock picks, which do not leave traditional marks, but still leave marks.

I have been doing my own research into anti-forensics materials and find that most of them are lacking in all areas. To date, no materials that I have tried have been successful at both picking a cylinder once and not leaving any forensic evidence. So far I have tried:

- Carbon Fiber
- Fiberglass
- Brass
- Teflon coated steel pick



These materials have also left various forensic evidence.

One area that anti-forensic materials may be used in is the production of non-metal keys. Plastic keys are considerably easier to use than plastic picks because their size is much bigger than the common lock pick. Research into this area is rather sparse, as well, with the use of a plastic pen casing to surreptitiously open low-security tubular locks being the most notable example.

Another area is "glue gun" shoulders for bump keys. Bumping can cause pronounced, noticeable damage to the face of the lock. This damage can be reduced or eliminated by removing the shoulder of the key and replacing it with a glue gun stick, an inexpensive piece of soft plastic. (Note: This technique does not remove the forensic evidence found inside the plug or on the pins.)

## Tryout Keys

Tryout keys are a surreptitious entry technique against pin-tumbler and wafer locks. They use a series of keys with varied cut and spacing configurations to exploit poor tolerances in low-security, master keyed, or extremely worn locks. A tryout key works by being inserted into lock and jiggled back and forth in order to attempt to align components at the shear line. To assess the effectiveness of tryout keys against a particular lock, 25 random keys for the lock are produced. The forensic investigator attempts to use these keys, inserting and jiggling them, to open the cylinder. The investigator can provide a reasonable assumption on their effectiveness based on how many were able to open the cylinder.

## Visual/Optical Decoding

Visual and optical decoding of the combination, key, or internal components is another form of surreptitious entry. In this case, observation, surveillance, photography, or optical devices are used in various ways. In all cases, a key can be produced with the information gathered from decoding:

- Observation of a key's bitting depths or direct code.
- Photograph of a key's bitting depths or direct code.
- Observation/surveillance of a combination lock sequence being entered.
- Visual decoding of a key impression.
- Visual decoding of a master key system through the analysis of system key(s).
- Optical viewing of component positions.
- Optical viewing of component shapes (Medeco Biaxial, for example).
- Optical viewing of component coloring (indicates depth).
- Thermal viewing of electronic keypads.
- Radiological imaging.

When we speak of optical viewing of components we're usually referring to invasive tools such as a borescope or otoscope.

There are several high-profile anecdotes which illustrate the power that visual decoding has. The Diebold company once published a picture of a key used for voting machines across the country on their website. This key (wafer) was visually decoded and it was found that it could be used to gain access to every single voting machine in the country. In the great story of the Antwerp Diamond Heist, thieves obtained the combination sequence by installing surveillance above the combination lock on the overhead alarm used above the safe door.

## Combination Manipulation

Almost all low-security combination padlocks and Group 2 safe combination locks are subject to compromise by manipulation. Manipulation may be seen as a method of decoding where diagnostic information is taken through the use of the combination dial in order to determine the proper combination sequence. Manipulation is commonly (though erroneously) portrayed in many films, and is indeed an effective method against many combination locks. Group 1 or Group 1R safe locks are considered "manipulation resistant" because of various design changes that limit the effectiveness or drastically increase the time required to successfully perform manipulation.

**Auto-dialers** (or computer dialers, robot dialers) are machines that automate the process of manipulation either through sophisticated manipulation software or brute-force cracking of the combination. Auto-dialers may leave forensic evidence depending on how they are mounted to the combination lock and how long it takes to work. The process of auto-dialing accelerates wear on the lock components, and this may be detectable. The use of rotary combination locks with an electronic audit log may also be able to spot and prevent this sort of activity.

## Radiological Imaging

Radiological imaging is a form of surreptitious decoding that uses penetrating radiation (X, beta, and gamma rays)

to "see" inside the lock or safe, revealing the proper positions of components. This is most often used against Group 2 rotary combination safe locks to determine the position of each gate in the wheel pack. This is a surreptitious entry technique unless the use of such a device can be detected. In many cases, even if the ability to detect this form of entry is available it may be considerably expensive. The KGB is widely known to have used these devices when compromising American safes during the cold war.

The use of low-density wheel materials (such as Delrin) combats this attack. Group 1R safe locks are specifically designed to defeat various radiological attacks as well as provide manipulation protection.

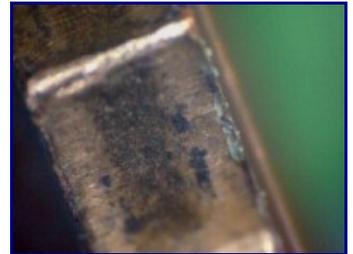
### **Surreptitious Bypass**

There are some forms of bypass that may be surreptitious if used properly. Most padlock bolt shims are made of metal, but some low-security padlocks are of a poor enough quality that they can be shimmed with paper. This, of course, does not leave marks on the padlock bolt.

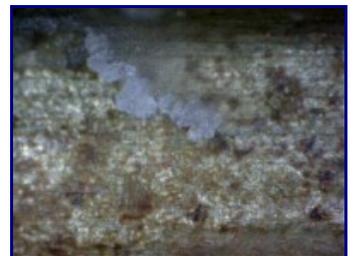
In the case of a thumbturn or lever (handle) lock, there are tools that will reach under the door and attempt to grab the thumbturn or handle and unlock or open the door. Depending on the design and material of the tool and the number of attempts it takes to open the door there may not be any forensic evidence. In this case, the forensic locksmith will note that the potential for this attack exists. If no other evidence is found it may be decided that this was one of the most probable methods of entry.

### **Material Transfer**

Various materials are transferred to the key during use. Generally hair, fiber, and fingerprints will be examined by a crime lab. The forensic locksmith, however, may examine the findings of the crime lab to identify the uses of materials found on keys. Here we see a light green residue, which happens to be modeling clay.



In this photo we find small traces of white wax left in the warding of the key. Both this and the previous image indicate that the key has been impressioned (via copying). Through further analysis we may be able to link these and other materials to those found in a suspect's possessions.



Keys should also be viewed under various light sources to attempt and fight any material residue that may not be visible with the naked eye (or naked microscope?). In this photo, a key is being viewed under ultraviolet light to discover traces of ultraviolet ink along the key biting area, indicative of impressioning via manipulation.



### **Bypass Principles**

Attacks against the cam or actuator are a class of bypass that is surprisingly effective. In this attack, a poorly designed cam or actuator may be manipulated without affecting components. This vulnerability is somewhat uncommon, but extremely effective and easy to do when present. Because tools must generate a mild amount of torque as well as travel through the plug, they leave distinct tool marks.

Spring loaded bolts or latches are subject to an attack known as shimming. In shimming, a wedge is used to separate the bolt from the spring, or the bolt from the recess (such as in a door). The classic credit card trick to open doors is a popular example of this technique. Low-security padlocks are also commonly susceptible to shimming of the shackle. Shimming against doors is also known as loiding.

Locks that use a thumb-turn or lever handle on the inside of the door may be vulnerable to bypass. In this attack a tool is slipped under the door and attempts to swing and catch onto the thumb-turn or lever. The tool is used to turn or pull until the door is opened. This may or may not have forensic evidence, depending on the material of the tool, handle, and how many attempts are necessary to gain entry.

In automobiles, the door frame may be attacked with what is known as a air wedge. First, a wedge (usually plastic) is used to lightly separate the door from the frame of the automobile, then a deflated air wedge is placed in the opening. The air wedge is filled with air, causing it to expand, and the door is held open to allow a tool to be inserted to manipulate the inner unlocking mechanisms inside the vehicle. This technique is commonly used by locksmiths during automobile lock-outs.

The American 700 (old models) have a vulnerability that allows bypass via manipulation of the cam. Essentially, the cylinder is not required to move in order to actuate the cam. Tool marks left on the cam and back plate indicate that bypass was used as the method of entry. In response to the above attack American Lock (now owned by Master Lock) issued a hardware patch to prevent the bypass method. It is just a small metal disc, and in the photo we can see tool marks from where bypass was attempted. The 700 has since been redesigned because another attack against this component makes bypass again possible.

### **Excellent websites on lockpicking**

<http://www.iail.org>

The International Association of Investigative Locksmiths

<http://toool.us>

The Open Organization of Lockpickers

<http://www.ndemag.com>

Free lockpicker / hacker magazine much like the Paranoid

<http://www.theamazingking.com>

Great website about cryptography and lockpicking

<http://www.deviating.net>

Lockpicking website

<http://blackbag.nl>

Lockpicking website

<http://www.lockpicking101.com>

Lockpicking website

<http://www.lockwiki.com>

Interactive locksmithing site with excellent beginners introduction.

### **Thank you for reading our tenth edition**

**Visit Resist.com to buy future and archived editions.**

### **Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**

# The PARANOID Newsletter

Because they ARE out to get you.

*By three methods we may learn wisdom: First, by reflection, which is noblest;  
Second, by imitation, which is easiest; and third by experience, which is the bitterest.  
- Confucius*

In a country well governed, poverty is something to be ashamed of.  
In a country badly governed, wealth is something to be ashamed of.  
- Confucius

## **Introduction**

This is the eleventh issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding fathers say if they were alive today!

## Safe cracking with thermal imaging technology

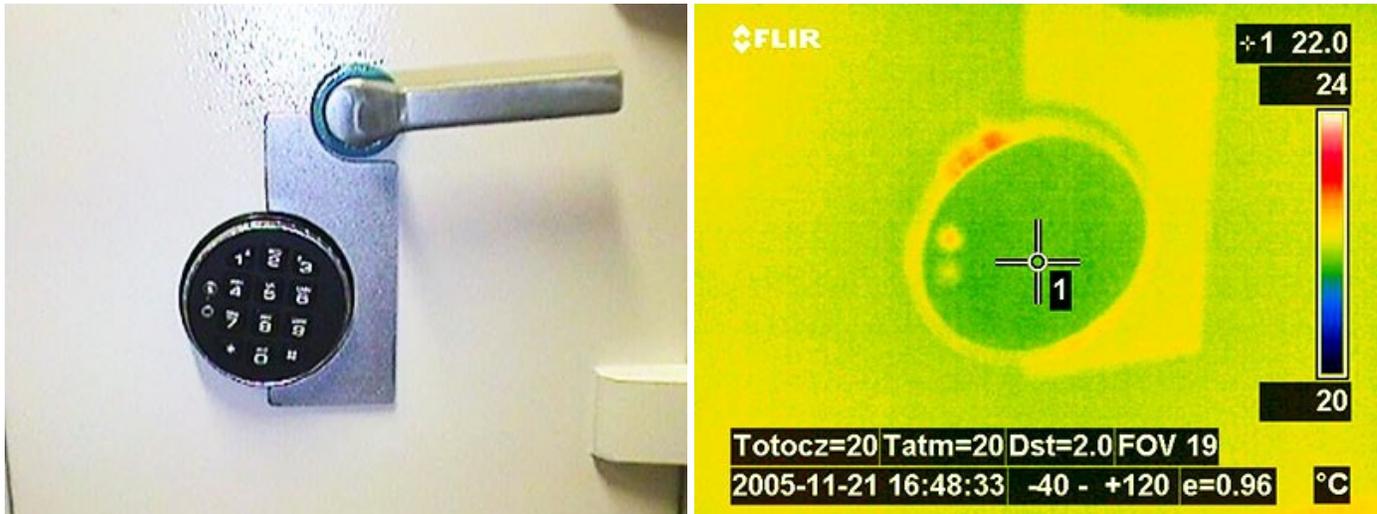
Virtually all keypad entry systems - as used in various applications, including building access control, alarm system control, electronic lock safes, ATM input, etc - are susceptible to a trivial low-profile passphrase snooping scheme. This attack enables the attacker to quickly and unobtrusively recover previously entered passphrases with a high degree of success. This is in contrast to previously documented methods of keypad snooping; these methods were in general either highly intrusive - required close presence or installation of specialized hardware - or difficult to carry out and not very reliable (e.g., examining deposited fingerprints - works in low-use situations only, and does not reveal the ordering of digits).

The attacker can perform the aforementioned attack by deploying an uncooled microbolometer thermal imaging (far infrared) camera within up to approximately five to ten minutes after valid keycode entry. Although this may sound outlandish, the heat transferred during split-second contact of individual keys with human body (even through, for example, gloves) is significant enough and dissipates slowly enough to make this possible after the area has been cleared of all personnel.

Furthermore, since the image can be acquired from a considerable distance (1-10 meters is easy to achieve), the attacker can afford to maintain a remarkably low profile through the process.

To put things in perspective, portable (handheld) thermal imaging devices, such as the one pictured above, are commercially available without major restrictions from manufacturers such as Flir or Fluke. Prices begin at \$5,000 to \$10,000 for brand new units, and top-of-the-line models boast a 0.05 K thermal resolution at impressively low sensor noise levels. The "return on investment" can be quite high in most illicit uses, and indeed - historically, ATM phishers were known to be willing to spend money on specialized equipment such as custom assemblies that included high-end digital cameras with wireless access. As such, the scheme is not as outlandish as it might have seemed.

The following sequence of images demonstrates the feasibility of the attack; in this case, the target is LA GARD ComboGard 3035 electronic lock (with rubber keys) installed on an industrial-grade safe:



Keypad in idle state - in visible light (left) and in thermal imaging (right). Minimal ambient temperature variations are present due to different thermal characteristics of materials used in the safe.



A sequence of keys is being pressed (1-5-9). The difference in colors on the right is due to IR camera automatically adjusting to relatively high temperature of human body, to avoid overexposure and blooming.



*Code entry complete. All pressed keys are still clearly readable in this thermogram; the sequence of digits can be inferred from the relative temperature of these spots - ones with lower registered temperature (more faint color) were pressed earlier than others.*

There are some real-world considerations, of course: reuse of digits in a code, very rapid code entry, vastly differing keypress times, and other code entry quirks (say, victim's habit of resting his palm on the keypad) may render the attack less successful, and may make results more ambiguous. That said, it's still nifty, and apparently not limited to bad science-fiction or computer games; civilian access to sufficiently advanced technology is possible. All in all, many airports, numerous bank branches, and various other entities, might want to reconsider the effectiveness of their defenses.

A proper defense against such techniques would be not to rely on keypad-only access control in easily accessible areas, unless additional advanced countermeasures can be implemented (well-implemented scrambling keypads originally intended to thwart fingerprint or key wear analysis, for example). Smart-card, biometric, or plain old key-based protection can be added to reduce exposure.

*Side thought: in terms of safe cracking, another interesting area of research is differential power analysis (DPA) of electronic locks. High-security locks on small- and medium-size safes usually have external connectors that can be used to supply emergency battery power to the device; these usually directly connect to the same route that is used to supply primary power, and as such can be used to measure power consumption characteristics and/or capture CPU-generated feedback noise, and possibly to differentiate between valid and invalid keycodes as digits are entered. If you happen to have a good 'scope lying around, give it a try.*

## Countermeasures

Place whole hand on keypad for several seconds to ensure the entire keypad is warmed. This can also prevent someone from placing dust, grease, or some other hard to see residue from returning and examining the keypad.

Scrambling keypads are more expensive but prevent these attacks without any additional user effort.

Use a glass rod to dial in your combination. (glass is IR opaque)

Use rotating dial locks.

# NSA continues surveillance of journalists

By Wayne Madsen  
Online Journal Contributing Writer  
[www.waynemadsenreport.com](http://www.waynemadsenreport.com)

On May 10, 2005, WMR reported on the existence of a highly-classified database at the National Security Agency (NSA), formerly code-named "FIRSTFRUITS," that monitored journalists who reported on the activities of the eavesdropping agency, as well as other intelligence matters. A few weeks later, according to an executive-level source at the NSA, and confirmed by a related source within NSA's "Q" Directorate, the Directorate for Security and Counterintelligence, this editor has been a subject of a national security investigation since June 2005 that remains ongoing. The investigation of this editor is classified at the level SECRET/COMINT (NOFORN). COMINT is "Communications Intelligence" and NOFORN denotes "Not Releasable to Foreign Nationals/Governments/Non-US Citizens."

According to National Security Agency/Central Security Service Policy 1-27, dated March 20, 2006, and signed by NSA Chief of Staff Deborah Bonanni, the investigation of the public disclosure of the unconstitutional and illegal FIRSTFRUITS surveillance system is being coordinated by the NSA, Department of Defense, Director of National Intelligence, and the Department of Justice.

The following are excerpts from the editor's article that triggered the national security criminal investigation: "*NSA maintains a database that tracks unofficial and negative articles written about the agency. Code named 'FIRSTFRUITS,' the database is operated by the Denial and Deception (D&D) unit within SID [Signals Intelligence Division]. High priority is given to articles written as a result of possible leaks from cleared personnel.*

*According to those familiar with FIRSTFRUITS, Bill Gertz of The Washington Times features prominently in the database. Before [NSA Director Michael] Hayden's reign and during the Clinton administration, Gertz was often leaked classified documents by anti-Clinton intelligence officials in an attempt to demonstrate that collusion between the administration and China was hurting U.S. national security. NSA, perhaps legitimately, was concerned that China could actually benefit from such disclosures.*

*In order that the database did not violate United States Signals Intelligence Directive (USSID) 18, which specifies that the names of 'U.S. persons' are to be deleted through a process known as minimization, the names of subject journalists were blanked out. However, in a violation of USSID 18, certain high level users could unlock the database field through a super-user status and view the 'phantom names' of the journalists in question. Some of the 'source' information in FIRSTFRUITS was classified -- an indication that some of the articles in the database were not obtained through open source means. In fact, NSA insiders report that the communications monitoring tasking system known as ECHELON is being used more frequently for purely political eavesdropping having nothing to do with national security or counter terrorism.*

*In addition, outside agencies and a 'second party,' Great Britain's Government Communications Headquarters (GCHQ), are permitted to access the journalist database. FIRSTFRUITS was originally developed by the CIA but given to NSA to operate with CIA funding. The database soon grew to capacity, was converted from a Lotus Notes to an Oracle system, and NSA took over complete ownership of the system from the CIA.*

*Tens of thousands of articles are found in FIRSTFRUITS and part of the upkeep of the system has been outsourced to outside contractors, such as Booz Allen, which periodically hosts inter-agency Foreign Denial and Deception meetings within its Sensitive Compartmented Information Facility or 'SCIF' in Tyson's Corner, Virginia. Currently, in addition to NSA and GCHQ, the National Geospatial-Intelligence Agency (NGA), the Defense Intelligence Agency (DIA), and National Reconnaissance Office (NRO) routinely access the database, which is, in essence, a classified and more powerful version of the commercial NEXIS news search database.*

*In addition to Gertz, other journalists who feature prominently in the database include Seymour Hersh of The New Yorker,; author and journalist James Bamford, James Risen of The New York Times, Vernon Loeb of The Washington Post, John C. K. Daly of UPI, and this journalist [Wayne Madsen].*

Since the disclosure of FIRSTFRUITS, NSA changed the cover name but the system remains in existence. Not only does the follow-on to FIRST FRUITS contain articles about NSA written by journalists, it has been expanded to include information gleaned from wiretaps on journalists, including sources with whom they communicate by phone, email, fax, and Voice-over-IP (VOIP), including Skype, which the NSA has managed to bring under easier surveillance due to some recent advances in VOIP surveillance technology, according to NSA sources.

This editor has, thanks to dozens of NSA sources, managed to report on the poor morale; overbearing Stasi-like conduct of NSA security personnel, including the wrongful prosecution and conviction of NSA Iraqi shop analyst Ken Ford, Jr.; contract mismanagement and fraud conducted by then-NSA Director General Michael Hayden; outrageous treatment of NSA whistleblowers by the NSA security and psychological staffs that work in the same fashion that the old Soviet KGB and psychiatric hospitals treated dissidents; and the outsourcing of sensitive signals intelligence contracts to companies with dubious links to foreign intelligence agencies, most importantly, those of Israel. Federal investigators are apparently using the terms “espionage” and “treason” with regard to the investigation that includes this editor. The maximum penalty for espionage and treason, according to U.S. Sentencing Guidelines, is death.

On January 12, 2006, this editor first reported on the criminal investigation being carried out by the Bush administration: *“Informed intelligence sources have informed this editor that he has, since October 2005, been under an active federal criminal investigation as part of the Bush administration’s probe of leaks about illegal NSA surveillance of U.S. citizens.*

*To reiterate what I’ve stated before: I refuse to cede my First Amendment rights and will not cooperate with ANY grand jury asking questions about sources and I will refuse to turn over notebooks or other materials to any investigators, warrant or not. I’m willing to become a political prisoner rather than succumb to the fascist thugs in the Bush administration. WMR is working on a number of investigations involving The Carlyle Group, the Fellowship Foundation, and illegal surveillance. We will continue to publish until the Bush administration makes their move to shut us down. Again, your support has helped us to gain enough of a media presence to make the Bush administration nervous.”*

This publication, not intimidated by NSA, the FBI, or other Bush administration entities, will continue to report on the misuse of America’s intelligence agencies for political purposes and the repeated violations of the U.S. Constitution by illegal surveillance of citizens, including First Amendment-protected journalists. WMR has learned today [Monday] that our colleague, New York journalist Joe Lauria, who has written a series of articles on the Turkish/Israeli intelligence network exposed by former FBI translator Sibel Edmonds, is now also the subject of an FBI “leaks” investigation.

The FIRSTFRUITS journalist surveillance system was renamed after our exposure of its existence. According to our NSA source, who was involved in another operation designed to scan the media and academia for leaks, a program called “Cryptologic Insecurities,” FIRSTFRUITS exists within a new strategic program by NSA to surveil journalists, which may be the subject of a classified United States Signals Intelligence Directive (USSID 304P), dated June 7, 2007. One term used by NSA with regard to journalists in the FIRSTFRUITS follow-on surveillance system is the Orwellian-sounding “media control.”

There is also reason to believe that additional journalists are now subject to FIRSTFRUITS surveillance and include Eric Lichtblau of the *New York Times*, Christiane Amanpour of CNN, and Lauria. WMR has also learned that NSA has drastically cut the number of Hebrew and Russian linguists, with the Hebrew linguists suffering the greatest cuts. The result of this decision is that the two languages used most by international organized criminal syndicates that are part of the Russian-Israeli Mafia are virtually free to conduct their weapons, diamond, and drug smuggling operations, as well as financial fraud, without being subject to NSA surveillance.

Perhaps the fact that there exists a cabal within the U.S. District for Maryland, a few officials who have conspired to wrongfully prosecute NSA employees is not coincidental to the purge of Hebrew and Russian linguists at NSA. A triumvirate has emerged that suggests illegal collusion to prosecute NSA whistleblowers that includes U.S. Attorney for Maryland Rod Rosenstein, his assistant David Salem, and US Judge Peter Messitte, who, according to U.S. intelligence sources, carries, in addition to his U.S. passport, a passport issued by Portugal.

WMR has also learned that an NSA signals intelligence mission codenamed "SALAMANDER" and devoted to monitoring communications in Georgia, may have been misused to provide the neocon Georgian government of Mikheil Saakashvili with intelligence gleaned from NSA intercepts of Saakashvili's political opponents, including alleged phone calls with Russian embassy officials in Tbilisi. Those targeted in the wiretaps include Labor Party leader Shalva Natelashvili, Freedom Party leader Konstantin Gamsakhurdia, the late Georgian opposition financier Badri Patarkatsishvili, and Conservative Party leader Zviad Dzidziguri. The provision of U.S. SIGINT to a nation like Georgia, which is well outside the normal American "second party" and "third party" SIGINT partners, represents a dramatic departure from traditional U.S. intelligence management and may have provided sensitive sources and methods information to the Georgian government, one which includes a number of dual Georgian-Israeli nationals.

## Review of Low noise .22 long rifle ammo

*Who needs a silencer with Aguila's .22 Sniper Subsonic 60 Grain quiet ammunition?*



At last count I had nineteen different types of .22 rim fire ammunition. Today, I have to make that an even twenty. Once again I have fallen to the curiosity of an offering previously unknown to me. This time it was, perhaps, the most unusual .22 rim fire I have seen. Aguila, a company not afraid to offer something different, brings us it's 'Sniper Subsonic' round with a 60 grain solid lead bullet. Yes.... 60 grains. The heaviest .22 rim fire normally encountered is 40 grains. Higher velocity rounds usually drop that to 36 grains, or even 30 grains.

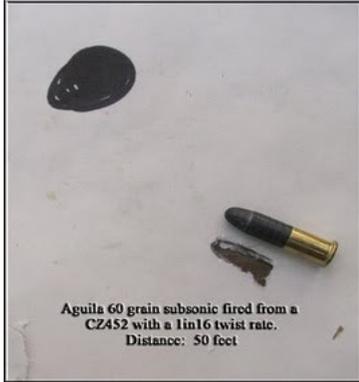


Aguila managed to squeeze that huge slug into a long rifle sized package by taking a unique route. They used a .22 short case, with a reduced powder charge, and loaded a very long lead bullet into it, bringing the whole cartridge out to .22 long rifle length. The SSS round looks the part too, with half the cartridge length being lead bullet. That's more than unusual, it's down right strange looking. The idea is fascinating, with the heavy bullet retaining substantial energy while the low velocity and charge give greatly reduced noise. The problem with this approach is one of bullet stability.



Heavier low velocity bullets require a rapid twist rate to stabilize the bullet in flight. Lighter high velocity bullets can use a slower twist rate to accomplish the same stability. Bullet design also comes into play in the equation. Even the type of rifling can have an effect.

Typical .22 rim fire firearms shooting a 35 to 40 grain bullet at 1000 fps work well with a 1 in 16" twist rate, and this is standard for these weapons. A .223 center fire shooting a 60 grain bullet at 3200 fps usually works well with a 1 in 9" twist.



A .22 rim fire shooting a 60 grain bullet at subsonic velocities? A rapid twist would be in order, and its doubtful that 1 in 16" will do it. The test is simple. Load an accurate .22 rifle with the new ammunition, sight on a reasonable target, and note the results. That is exactly what I did, and the results are shown here.

The rifle chosen was a CZ452 Trainer, and is exceptionally accurate. It has shown a tolerance for various cartridges, without being overly picky about what it will shoot well. The long barrel and deep rifling may have something to do with that, as well as the tight bore. This rifle, even with open sights, constantly surprises shooters with it's consistent ability to group tightly.



Setting simple 4"x6" card stock targets at 50 feet, several rounds were fired. Only a were needed to answer the basic question. The very first round was a classic keyhole, as was every round after. The Aguila 60 grain bullets simply would not stabilize in the 1 in 16" twist CZ barrel.

Fired at both a paper target and a block of pine, the imprints are clear sideways impacts of a bullet tumbling in flight. Perhaps this ammunition would be better suited to a .22 wearing a custom rapid twist barrel, as many folks have fitted to Ruger 10/22s. Also, it might be a perfect round for an AR equipped with a rim fire conversion, especially if it has a suppressor can installed. For my .22's, all of which have 1 in 16" twist barrels, I'm afraid this Aguila offering is useless.

### **22LR 20gr Aguila Colibri**

Solid no powder charge. Use only in handguns! Even quieter than Super Colibri. Perfect ammo for teaching a youngster with a .22 LR revolver. Sounds like a loud airgun when fired.

### **22LR 20gr Aguila Super Colibri**

20-gr Solid, no powder charge, 500 fps. Use only in handguns! Perfect ammo for teaching a youngster with a .22 LR revolver. Sounds like a loud airgun when fired.

### **22LR 32gr Segmented HP Hyper-Velocity**

Manufactured in the USA by Blount (CCI) for Magnum Performance Ballistics. Muzzle Energy 149 ft-lbs, Muzzle Velocity 1,367 FPS 32-gr .22 Long Rifle (LR) The bullet split into 4 main segments on impact. These segment cause 4 separate wound channels. Great for small game and self-defense pocket pistols. 1/2" groups at 50 is not uncommon.

## **Comments from a .22 LR hunter**

I have a few boxes of Eley 22 CB/wadcutter shaped caps left. From two of my rifles and three of my handguns they are very good...accurate from very fine, to minute of squirrel head at 25 yards. From the rest of my 22s they are stinkers. If I hadn't tested them in those guns only, and didn't know that 22RF ammo is generally like this, I would have thought the stuff was just no good. Moral of the story...test ammo in as many 22RF guns as you can...and before you pronounce any new 22RF gun or ammo inaccurate, try a number of brands in a your guns if

possible, till you find the combination you likes best....Rem C.B. Caps, Subsonic Remington, Aguila (no powder), Wolf Performance Match, Aguila Super Extra shorts and long rifle, Yellow Jacket Remington, Win Power Point, CCI Quik Shok, Remington Cyclone, Aguila 22-SSS, Remington Subsonic, CCI Stinger, Remington Thunderbolt. One thing that did become very apparent, when the 22RFs (no matter what brand) were ACU'RZED the velocity went up. A little with some brands like the subsonic types, and a good deal with the high and hyper velocity types. What the ACU'RZING does do with the subsonic types is vastly improve their accuracy, Aguila's no powder rounds for example actually grouped from the Colt... where they won't with out ACU'ZRING.

As far as hunting with 22RFs goes for me...I don't. I will use them for exterminating small vermin, garbage birds, and a quail or two on occasion for the pot. But for the most part, I use loaded down centerfires on any animals over a several pounds or more. That is personal choice on my part...you may rightly feel differently. And with that, I also think range and nose shape have more to do with 22RF killing power than most realize.

For a very extended period I and a number of friends, we worked at four position 22RF (among other calibers) rifle target shooting in NRA matches...as well as NRA handgun matches....I have no idea how much 22RF ammo I have burned in contest, practice, plinking and vermin...but it is quite a lot I'm sure. For a one year period in 1972 getting ready for National Matches at Camp Perry, I fired a minimum of one brick of 22RFs a week for a full year. I test a goodly amount of ammo every year.... since I put the ACU'RZR on the market, I have increased with a lot of 22RF shooting, in testing the tools and such.

I have used a number of CB caps. Most of them are silent in 22 rifles. And very low in sound from decent length handgun barrels. The Eley wadcutter shape in dry phone books penetrates the best with near 550 pages. The Aguila 'No Powder 22RFs' penetrated the lest at 320 pages...and CCI CB caps came in at 412 pages from rifles. Out of handguns the Aguila was the quietest...CCI had a snapping sound and Eley sounded like a kid's cap pistol. Again accuracy seemed to have more to do with the gun's appetite than anything else. Though if I had to prioritize, Eley would be first in everything...accuracy, power, excellent nose shape...Aguila next for accuracy, it's 20 grain bullet is pointed so in pest flesh it does quite well, and the CCI last.

Strange as it may seem, Aguila's SniperSubSonic ammo with it's 60 grain bullet and much more power, sounds about the same as CB caps from handguns. And it doesn't drop from the point of aim out to 25 to 40 yards like the other CBs do. And carries a great deal more energy. When CBs, Subsonic and such are ACU'RZED the diameter of the bullet is enlarged giving better accuracy because they come out of the tool perfectly round, but also the extra friction ups the velocity and striking energy.

The Aguila 'No Powder' ammo has something else going for it, it is in long rifle cases...I like that...less fouling in the 22 chambers. CCI makes a CB cap long, I had no luck with it in anything. Certainly the noses I reformed and others on the CB caps had a very noticeable change in killing power on garbage birds. I don't like Starlings, they have very bad habits and are very dirty birds, they carry a variety of diseases that hurt house hold pets more than people. Their only reason for existence is for bullet testing.

We had an Irish Setter when we were living in the wilderness years ago. He was wonderful, but really past his age for bird hunting anymore. He was in his sunset years...so when I would take out a rifle he would get all excited like bird dogs do, but his heart wasn't really in it. One day he was out in the back of the house and I shot a nasty starling off an electric power line. Ol'Mike saw the bird fall, his instincts kicked in and he looped as best he could to the downed bird, scooped it up in his mouth, turned to run back to me. Stopped suddenly....dropped the bird, looked down at it, and then vomited all over it!!!!

I always try to keep a supply of CB caps on hand...a good supply. Never know when you need a silent load. I have a trick I use to get rid of the neighborhood cats from coming in and fouling the property. I really don't want to hurt them, just dissuade them from returning. I call it "tail nipping". Using a scoped rifle I have set for close range...I hit them right on the tip end of the tail with a CB. They rarely come back for seconds, the damage is slight...they lick it clean and it heals Quikly...but the lesson is learned. The new "No Powder" Aguila caps are great for this, because they are so low powered and silent. At a sedate 405 fps from the rifle they only generate around 8

pounds...a little better than an air rifle load. From the 6 inch handgun they went 432fps.

Remember 22RFs reach their peak velocity in 16 inch barrels. With CB cap type loads that is most likely closer to 10 inches. So out of my 24 inch rifle they actually showed almost 30 fps less velocity all without ACU'RZING. Once they are reformed the velocity goes up. CCI CB caps went 600 from the 2 ½ inch barrel, and 758 from the 6 inch Colt, and 809 from the 24" rifle. From an old 16 Ithaca single shot they went 888 fps. Very silent from the rifle...as all CBs seem to be. WW's CBs went 556 from the little autoloader, 650 from the 6 inch Colt and 719 from the 24 inch barrel. Aquila's SSS ammo with it's 60 grain bullet does 665 from the 2 ½ inch, 826 from the Colt and 950 from the rifle. And with that bullet weight it is the best killer of the quiet to silent loads. Giving 120 foot pounds of muzzle energy from the rifle and 90 lbs from the Colt.

I test the expansion and killing properties of 22RFs by firing them into ice. I fill an old plastic milk jug or three liter soda bottle with water and freeze it. Most 22s will stop in them and you can see how they perform, the energy dispersion is very easy to see. And after the water melts, you can recover the bullet. And compare the performance. I write on the plastic bottle what bullet/ammo is in them, if I am testing a number of ammo types with a number of bottles, (alas, short term memory when you get old is untrustworthy). This doesn't mean that's how they will react in vermin and varmints... it is just a comparison between standard shapes and the ACU'RZED shapes for maximum potential performance.

Aguila must use pure lead, the no powder load called the Aguila Super Colibri, after hitting the ice lost only a grain in weight. As you can also see by the photo, the 60 grain bullet is so long that Aguila uses the short case to keep the over all length of the 22 long rifle, so it will function thru long rifle actions. Works fine in most of my auto pistols...up to a point. The same with two of my rifles...but if the rifling isn't fast enough accuracy goes out the window...remember you are using a bullet that is over 33% longer and a velocity that is very low. In my CZ rifle and my Anschutz Mod. 64 Silhouette heavy barrel it goes into very small groups...in my Rossi pump it goes sideways at 25 yards...you have to test. This SSS ammo is called subsonic...and that is exactly what it is...not silent, but quiet. It is the bullet's weight that makes it a fine short range killer of vermin. I like it better ACU'RZED than the CBs, unless I need total silence.

## Mafia Hitmen, .22 caliber killers.

It seems improbable that a brotherhood as violent as the Mafia is becoming still more savage. It also seems unlikely that teams of professional hit men armed with silencer-equipped .22-cal. automatic pistols are roaming the land, with at least 20 "executions" to their credit in the past two years. Finally, it seems unthinkable that the case of the .22 hits could be a direct challenge by the Mob to the U.S. Government.

But the FBI fears all this is true, with good reason. Two of the victims were FBI informants. Four others were potential prosecution witnesses. Two of the killings — five months apart — were committed with the same gun. Says an FBI agent: "Keeping a murder gun is risky business. The Mafia has a reason for doing that. They're giving us a message."

Mafia Hot Line. Detective fiction has it that the .22-cal. pistol with its tiny one-ounce slug is a gnat swatter, at its worst a woman's weapon snatched from a purse to dispatch an errant lover. No self-respecting all-pro killer would carry one. The facts, however, are otherwise. The CIA has long preferred the .22. The agency's predecessor, the Office of Strategic Services, developed a silencer-equipped Hi-Standard .22-cal. automatic pistol during World War II. It turned out to be the only production-model handgun that can be effectively silenced, and it has been the favorite of spooks ever since. Now, says the FBI, the .22 has found new fans.

The Mob's change in execution methods is exemplified by February's killing of Mafia Consigliere Frank ("Bomp") Bompensiero, 71. Shortly before 8 p.m. on Feb. 10, Bomp walked from his San Diego home to a nearby public telephone booth, which he used as an office in order to avoid wiretaps. In his pocket was a notebook

containing coded balance sheets of loan-shark usury payments and lists of coded phone numbers. The numbers turned out to be those of other public telephones scattered through California and Nevada. The phones constitute a West Coast Mafia hot-line system.

At designated hours on specified days, Bomp would call a San Francisco number to chat with a sidekick named Jimmy Fratianno; at other times he would dial a Las Vegas booth for messages from Tony Spilotro, a Chicago gang heavyweight. He also received calls at the booth. A Mafia member for 40 years, Bomp was a consequential figure in the Mob hierarchy. He was also an informant for the FBI, the highest-placed Mafioso in that role.

The FBI has no idea whom Bompensiero telephoned that night, but they know one of his callers fingered him for execution. The old man was an easy target. As he walked away from the phone booth toward his home, he was dropped by a .22-cal. slug that entered his neck near the spine. The coup de grâce was a second shot near the right ear. No shots were heard. When the body was found, the notebook was missing. Nineteen other victims are listed by the FBI in the case of the .22 hits. Almost all were dispatched with multiple shots to the head from a .22-cal. automatic pistol. All had in some way crossed the Mob. The most noteworthy:

Sam Giancana, 66, retired Mafia boss, who was shot in the basement of his Chicago home in June 1975. Investigators believe Giancana was slain for refusing to share the take from Caribbean gambling ships, a fringe benefit that he acquired in the early 1960s.

Jack Molinas, 43, master fixer of college basketball games in the nationwide point-shaving scandal of 1961, and later the producer of hard-core sex films. He was shot in the head in his Hollywood Hills home in August 1975 for cheating Mafia loan sharks.

Tamara Rand, 54, San Diego businesswoman, murdered at home in November 1975 to keep her from telling what she knew about Mob-dominated gambling casinos in Las Vegas.

Edward Lazar, 40, accountant and mortgage-company president, gunned down in February 1975 in a Phoenix parking garage the night before he was to appear before a grand jury investigating land speculation.

Augie Maniaci, 66, Milwaukee swindler, who was executed in September 1976 in an alley behind his home. Maniaci was an FBI informant.

Vincent Capone, 39, a small-time gambler and loan shark slain in Hoboken, N.J., in August 1976 while his Cadillac was stopped for a red light. Two killers hit him with 15 shots. He was reportedly about to turn state's evidence in an investigation of New Jersey Mobster John DiGilio.

Frank Chin, 48, professional wiretapper gunned down with six bullets to the head in a New York City apartment building Jan. 20. Also a potential state's witness against the Mob, Chin (TIME, Feb. 21) had been hired by DiGilio to screen the gangster's offices for police eavesdropping devices.

Arthur Milgram, 48, head of a company that sells New York State lottery tickets through vending machines, executed on Feb. 8 in a Queens parking lot. Milgram was reportedly about to squeal on Mafia loan sharks who were trying to take over his business.

The grim prospect of a professional coast-to-coast gang methodically exterminating potential court witnesses and FBI informants has led the bureau to assign agents in 20 field offices to the case. Findings so far have strengthened the FBI'S hit-team suspicions. Two .22 pistols discarded after killings were traced to a Miami sporting-goods store that went out of business a few months ago. FBI lab tests show that the .22-cal slugs that killed Capone and Chin came from the same weapon—which has not been found. But both men were also linked through their mutual connection with DiGilio. The New Jersey gangster is currently appealing a prison sentence for conspiracy to rifle the files of the FBI's Newark field office—files that some officials think may have tipped off the Mob that Bompensiero and Maniaci were informants. The identity of the hit men is a mystery to most of the Mafia too. Some Mob insiders believe they are a squad of "greenies"—gunmen lately brought illegally into this country

from Sicily. Others say the .22 hits are the work of young Viet Nam War vets. Still other sources pin the killings on two seasoned triggermen of New York Drug King Carmine Galante. Whoever they are, they have brought the silenced .22 loud notoriety.

**Thank you for reading our eleventh edition**

**Visit [Resist.com](http://Resist.com) to buy future and archived editions.**

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**

# The PARANOID Newsletter

Because they ARE out to get you.

If you know the enemy and know yourself,  
you need not fear the result of a hundred battles.

If you know yourself but not the enemy,  
for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself,  
you will succumb in every battle

- Sun Tzu

## Introduction

This is the twelfth issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding fathers say if they were alive today! This twelfth edition of the paranoid newsletter discusses white racists developing weapons of mass destruction and explosive taggants.

## Terror Anthrax linked to type made by U.S.

By WILLIAM J. BROAD

December 3, 2001

**The dry powder used in the anthrax attacks is virtually indistinguishable in critical technical respects from that produced by the United States military** before it shut down its biowarfare program, according to federal scientists and a report prepared for a military contractor.

The preliminary analysis of the powder shows that it has the same extraordinarily high concentration of deadly spores as the anthrax produced in the American weapons program. While it is still possible that the anthrax could have a foreign source, the concentration is higher than any stock publicly known to be produced by other governments.

The similarity to the levels achieved by the United States military lends support to the idea that someone with ties to the old program may be behind the attacks that have killed five people. The Federal Bureau of Investigation recently expanded its investigation of anthrax suspects to include government and contractor laboratories as a possible source of the deadly powder itself, or of knowledge of how to make it.

**Its high concentration is surprising, weapon experts said, and far beyond what military analysts once judged as the likely abilities of terrorists.** Still, experts caution that the emerging evidence is tentative and that it is too early to rule out other possible suspects, be they **domestic lone wolves** or hostile foreign states

like Iraq.

A yardstick for measuring the quality of anthrax emerged almost three years ago when William C. Patrick III, a longtime federal consultant and one of the nation's top experts on biological weapons, wrote a report assessing the possible risks if terrorists were to send anthrax through the mail. Based on the difficulty of developing advanced anthrax, he predicted that the terrorist germs would be one-twentieth as concentrated as what the government developed and what has recently turned letters into munitions.

**"The quality of the spores is very good,"** said a federal science adviser who shared the Patrick report with The New York Times. **"This is very high-quality stuff"** — equal, he said, in concentration to that produced by the United States military before it abandoned germ weapons. The high quality lends credence to the idea that someone with links to military laboratories or their contractors might be behind the attacks. **"It's frightening to think that one of our own scientists could have done something like this,"** he said. "But it's definitely possible."

He said the anthrax sent to the Senate contained as many as one trillion spores per gram, a figure confirmed by an administration official. A gram is just one-twenty-eighth of an ounce. Yet in comprising up to one trillion spores, a gram of anthrax powder has vast potential to kill. If a lethal dose is estimated conservatively at 10,000 microscopic spores, then a gram in theory could cause about 100 million deaths. The letter sent to Tom Daschle, the Senate Democratic leader, is said to have held two grams of anthrax — enough, in other words, to make about 200 million lethal doses, assuming it could be distributed to victims with perfect efficiency.

Analysis of the Daschle powder has been hampered by the small amount recovered after an aide opened the letter, and by technical missteps as the investigation got under way, making some conclusions iffy. That is why investigators are taking great care in opening the anthrax-contaminated letter sent to Patrick J. Leahy, chairman of the Senate Judiciary Committee. The aim is to scrutinize the evidence as closely as possible.

Spore concentration is just one factor experts will examine in the Leahy letter, and their findings could significantly alter their picture of the powder. Other **factors that reflect the quality of anthrax production include** whether the powder has been **ground to a size that easily lodges in the lungs** and whether it has been treated to make it **static free and free-floating**. Investigators will look for **antistatic additives** that might be a possible hallmark of a particular government's weapons program. (Thanks for the tips!)

Mr. Patrick, in his risk assessment, sketched out both what the American military achieved and what a terrorist might do. His 28- page report, dated February 1999, was written for a federal contractor advising the government on how to handle the growing number of anthrax hoaxes and what to expect if real anthrax were to be sent through the mail. When these hoaxes first came up, **we assumed none of the bad guys could achieve high-grade anthrax,** said a contractor official, who spoke on the condition of anonymity.

It is unknown publicly exactly how makers of anthrax weapons achieve high spore concentrations, but the black art is said to involve precise drying, sifting, milling and removal of impurities. In his assessment, Mr. Patrick drew on personal knowledge acquired while working in the nation's offensive biological weapons program from 1951 to 1969, when it was dismantled, at which time he was chief of the division of product development. He won five patents with his colleagues for ways to make biological weapons.

His 1999 report focused on what kinds of contamination terrorist anthrax would cause when a letter was opened and what the requirements for decontamination were. Mr. Patrick postulated that the concentration of anthrax would be 50 billion spores per gram. "This assumes a dried powder of moderate ability to generate into

an aerosol when the envelope is opened," he wrote. He predicted that an envelope would hold 2.5 grams of anthrax — an amount strikingly close to what is thought to have been mailed to Senator Daschle.

In his report, Mr. Patrick said the American program had achieved a concentration of one trillion spores per gram — what scientists today say is near the theoretical limit of how many of the microscopic spheres can be packed into a tiny space. Today, no terrorist or scientific maverick is known to have published anything that comes close to describing how to make concentrated anthrax powders. **Timothy W. Tobiason, a habitué of gun shows who sells a self-published cookbook on how to make germ weapons, including "mail delivered" anthrax, sketches out only the most rudimentary steps. The book series is titled "Scientific Principals of Improvised Warfare" Volumes 1-6.**

Experts judge Mr. Tobiason's recipes as flawed in spots and at best capable of producing only low-quality anthrax. His book deals mostly with the production of wet anthrax, though it does suggest a way to grind clusters of dried anthrax into microscopic pieces, which can settle into the lungs. It is unclear if any foreign nation has achieved high anthrax concentrations. The United States suspects that more than a dozen countries are clandestinely studying biological weapons, with anthrax among the top agents. Ken Alibek, a former top official in the Soviet germ weapons program who is now president of Advanced Biosystems, a consulting company in Manassas, Va., said that it was routinely possible to create dry anthrax that contained 100 billion spores per gram and that, with some effort, 500 billion was possible.

"The infectious dose," Dr. Alibek said, "can be quite large." Still, the 500 billion figure is half the concentration that the American government and whoever sent the letters are said to have achieved. "I don't think they're manufacturing this in caves," Dr. Alibek said of the terror anthrax. "It's coming from another source." Lone wolves perhaps?

### **ADL Book Review**

Courtesy of the Anti Defamation League, the following books have been described in their briefings. After reading their descriptions, who WOULDN'T want to read them!

#### **The Poor Man's James Bond**

Survivalist guru Kurt Saxon is the author of *The Poor Man's James Bond*, a work similar to Benson's *Encyclopedia*. Such books not only explain how to build bombs and explosives; they also often discuss the manufacture of chemical and biological agents. Saxon, for example, has explained the manufacture of ricin in his books and videotapes.

#### **Silent Death**

*Silent Death*, a book written by "Uncle Fester," provides even more detail. "Uncle Fester" — actually Green Bay chemist Steve Preisler, a convicted criminal who wrote one of his books while in prison — describes himself as the "world's foremost clandestine chemist." His book is for the "home or clandestine manufacture of poisonous materials, with an emphasis on guerrilla war applications. Topics covered in *Silent Death* in detail include nerve gases, ricin, botulin toxin, and much more." **The Japanese cult Aum Shinrikyo, who launched a poison gas attack in Tokyo's subways in 1995, had copies of Preisler's book.**

## **Careless Talk gets Right Wing Yahoo's LONG prison sentences**

*Learning from the mistakes of others*

Two members of one South Texas faction of the sovereign citizen group known as the Republic of Texas, Johnie Wise and Jack Abbott Grebe, received 24-year prison sentences in 1999 for sending threatening e-mails to various federal agencies. They were acquitted of charges of planning to develop weapons of mass destruction (a third person was acquitted on all counts). This charge centered on discussions by the two men to modify a cigarette lighter to eject a cactus needle that would be coated with some sort of biological agent such as HIV, rabies, botulism or anthrax. According to an informant, the device would be used against the families of government employees. Although the Republic of Texas members had discussed developing rabies or anthrax for use in this fashion, they never actually made the device, nor is it clear that they would have proceeded with the rather far-fetched idea.

*Why wasn't this a one man operation? Why goto jail for threats? TRUST NO ONE!*

## **Dummies posses bioweapon for three years before betting busted**

*Learning from the mistakes of others*

Members of an anti-government group known as the Minnesota Patriots Council produced a quantity of ricin in 1992 to assassinate a U.S. deputy marshal and a deputy sheriff. The assassination was never executed. Three years later, Leroy Wheeler, Douglas Baker, Dennis Henderson, and Richard Oelrich-were arrested and convicted of “possession of ricin for use as a weapon” and given short sentences. They had learned about the poison from commercially available how to books on poisoning.

*Why were these dummies sitting on illegal Ricin when they no longer needed it?*

## **White racists have a proud history of cooking up WMD's.**

In the early 1970s, Muharem Kurbegovic, a Yugoslavian-born terrorist who sent toxic chemicals through the mail to a Supreme Court justice and threatened to use nerve-gas devices against the Capitol and the president of the U.S. He was arrested in August 1974 for a bombing that killed three people at the Los Angeles International Airport; following the arrest, police searching his California home found that he had all the ingredients necessary to construct a nerve-gas bomb.

The Covenant, the Sword, and the Arm of the Lord survivalist group from Missouri whose members belonged to Christian Identity were raided in 1985 and were found with a 30 gallon drum of cyanide.

In 1972, police arrested two teenagers, Steven Pera and Allen Schwander, who had started a small group called R.I.S.E. New recruits to the group tipped off police, who discovered that Pera and Schwander actually had typhus bacillus. The two teenagers skipped bail and fled to Cuba.

In April 1997, an anthrax hoax was directed at the international headquarters of B'nai B'rith, the well-known Jewish organization, in Washington, D.C. B'nai B'rith received an envelope in the mail that contained a petri dish with an unknown substance and a letter that statements aimed at Jewish liberalism and the Jewish community, as well as a reference to anthrax. The reaction by police was swift but harsh: four B'nai B'rith employees were taken outside, stripped to their underwear, and decontaminated with a bleach-water spray in full

public view in front of photographers. Meanwhile, more than 100 other employees were quarantined in the building for eight hours until authorities decided the substance was not dangerous.

Dr. Gordon C. Oehler, Director of the CIA's Nonproliferation Center, testified to Congress that "extremist groups worldwide are increasingly learning how to manufacture chemical and biological agents, and the potential for additional chemical and biological attacks by such groups continues to grow".

### **Robbing banks the intelligent way.**

*Really intelligent people don't steal in conventional ways.*

This is a much more "low key" way of stealing from a bank and will draw much less attention to you than a standard robbery would since, often, the bank won't publicize the theft, lest the other customers realize just how weak bank security is. Additionally, successful depository trap thefts are exceedingly rare, with only a dozen or two every year, compared to the thousands of standard style robberies. This is the pinnacle of the robbers art, to steal the money before it ever gets to the bank, and without anyone even knowing they've been robbed!

A depository is where people go to at the bank to drop off money without going inside, usually at night or when the bank is closed. A bank customer uses a key to unlock the depository chute, into which they place their money bag. When they close the chute, the money drops into a safe inside the bank. The chute is designed to resist forced entry to the same degree as the safe itself. And if someone left the chute unlocked, you wouldn't be able to retrieve the money by "fishing" for it because the chute has two intermeshed drums (like gears) that'd cut any line.

There is one occasion of this crime that has received widespread publicity in the past. In Japan, during the 80's, someone make an exact duplicate of a banks depository, and placed it over the original. Apparently people were too stupid to realize that the depository was now a good foot further than it was before, but that's neither here nor there. Point is, people put their money in the duplicate, which was emptied out afterwards by the criminal in readiness for the next victim. The thief scored more than \$300,000 in one night and was never caught. He also never repeated the crime, thus there was no pattern for the police to try to catch him with.

## **Recent unclassified Lone Wolf missions**

### **Switch-a-roo technique gives racists access to mainstream print media.**

New York, NY, December 21, 2009 In an effort to lure young people into the white supremacist movement, neo-Nazis are using deceptive new tactics to appeal directly to high school and college students through advertisements in their school newspapers. Neo-Nazi Kevin McGuire of Bozeman, Montana placed advertisements in school newspapers offering "free music downloads." In November, 2009 unsuspecting students at high schools in San Francisco and Carmel, Indiana were tricked into running ads promoting the racist "Victory Forever" site operated by McGuire.

The Victory Forever site initially displayed a page of music by independent artists, including at least one nigger musician. However, between the time when the ads were purchased and when they actually ran, the site was changed to promote racist material. "While the hatemongers have used stealth tactics before, now they are

taking it to the next level by attempting to trick unsuspecting students into logging on to sites that appear harmless, but in reality are promoting music with a white supremacist message," according to the ADL. Clearly "switcharoo" tactics are effective and content can be changed as soon as newspapers are printed and delivered to evade censorship. The website victoryforever.com is also selling skinhead music CD's for the rock bottom price of 25 for \$10 USD to promote distribution.

### **Five Poles destroy "Arbeit Macht Frei" sign at Auschwitz**

New York, NY, December 18, 2009 Five lone wolf Poles steal and destroy the "Arbeit Macht Frei" sign from the former death camp Auschwitz. The iron sign was stolen early Friday morning after having been unscrewed and ripped from its moorings at the memorial site in southern Poland. The sign was cut into three pieces, each containing one of the words Arbeit Macht Frei and scattered. The theft was carefully carried out and the lone wolves completely avoided attracting the attention of night watchmen or security cameras. The sign was removed through a hole in the camp fence before being loaded into a van.

**So what are YOU doing for the white race?**

### **Traditional ATF stereotyping of bombers (from a 1980's publication)**

The bomber population of the United States is extremely heterogeneous, with varying motives, resources, skills, and ability to adapt to a changing control environment. For ease of discussion, bombers are divided into four categories which differ from each other in most characteristics. These categories include terrorists, common criminals, the mentally disturbed, and vandals and experimenters. The characteristics of the various types of bombers are described

The terrorist groups active in the United States vary widely in ability, resources, training, and adaptability. They share the common characteristics, however, of high motivation, action as a part of a group, and a continuing involvement in catastrophic, illegal activities against society. These characteristics activities make the terrorist particularly dangerous to society and a particularly appropriate target for anti bombing controls. Terrorists can be roughly divided into political, reactionary, and separatist groups. Political groups are primarily interested in attracting attention to, and sympathy with, their cause. For that reason they engage in spectacular events, such as bombings, but generally attempt to avoid or limit injury and death resulting from their bombings. Political terrorists often have considerable resources available to them, due to the significant number of people who support their aim, if not necessarily their means. The leadership of most of these groups are of above-average intelligence, and have either had specialized training or have studied extensively in terrorist activities. They are thus able to adapt to a changing environment, although the range of responses available to them may be limited by their political aims.

Reactionary groups, such as the Ku Klux Klan and the American Nazi Party, share some of the characteristics of the political terrorists, but generally do not possess the same levels of training, motivation, and resources, and are not as capable of reacting effectively to a changing control environment. They also differ in that their bombings are usually directly targeted at the individual or group they intend to influence, rather than simply at a spectacular target.

*Lone wolves are highly motivated and highly educated, good luck dealing with them :-)*

## **ATF Tips for removing taggants from explosives and gunpowders**

In order to remove a nonmagnetic taggant with an opaque encapsulant from an explosive, the explosives could be acetone dissolved, the taggants and other Solid material removed by filtering, and the explosives reconstituted. This complex operation would require specialized knowledge, be roughly equivalent in danger and difficulty to fabrication of explosives from raw materials, and would result in less reliable explosives. *This is actually safe, easy, requires only solvent and a coffee filter. There is no loss of reliability or potency.*

Taggant removal from some gunpowders could be significantly easier than from explosives, as some gunpowder grains are considerably larger than the identification taggants. Separation from these powders may therefore be accomplished simply by screening, even if the taggants are nonmagnetic. Tests with several Du Pont IMR powders have shown that it would be difficult to separate the taggants from the chips and fines contained in the gunpowder package, but all small particles could easily be separated from the intact grains by screening. It has been proposed to alleviate this problem by agglomerating the taggants into clumps whose size roughly matches the specific powder grain size.

Fabrication of explosives may be accomplished by a variety of means, but a considerable degree of expertise is required to avoid the risk of premature detonations, and to ensure high reliability. It should be noted that fabrication of detonators is significantly more difficult than fabrication of the explosive charge.

*Keep telling yourself that ATF. Teenagers are building explosives from SCRATCH and are doing just fine.*

The effectiveness of detection taggants can be severely limited by creating a seal between the explosives and the detection taggant sensor as the vapor could not escape the package to trigger the sensor. Such a seal can be constructed with the appropriate industrial materials and equipment, but a reliable seal would be very difficult to fabricate with the resources normally available to individuals. Hence specialized knowledge, advance planning, and the resources to buy the required material, would be needed to defeat the detection taggants.

*So machines that vacuum pack and seal your food in a plastic bag can't seal your C4 + blasting cap?  
Rubbing alcohol can't be used to clean off residue on the outside of the sealed bag all of a sudden?*

Criminal bombers would fail to make use of countermeasures, even when the necessary knowledge and equipment could be obtained without enormous efforts. However, some terrorists and professional criminals would make use of countermeasures. This judgment is based on an assessment of the type of personality that is generally involved in this kind of criminal activity.

### **3M COLOR-CODED TAGGANT**

More research has been conducted with the 3M identification taggant than with any other. It is the baseline taggant proposed by BATF for implementation if a taggant program is legislated, and is the taggant used for the OTA cost, safety, and utility analyses. The taggant consists of an irregular chip of thermosetting melamine alkyd, approximately 0.12 mm thick and about 0.40 mm in its greatest dimension. Figure 6 shows the eight-layer construction; variation of the sequence colors provides the necessary library of codes. A total of approximately 6 million unique codes is available, when allowances are made for certain forbidden adjacencies (colors too difficult to distinguish) and other restrictions. One face of the taggant visibly fluoresces when

illuminated with black light (366 nanometers) as an aid in recovery, either in the field or laboratory. The other face contains iron powder, allowing the taggant to be picked up by a magnet, another recovery aid.

In theory, the taggant can be recovered from the debris by use of a magnet and a black light, read in the field by a low-power microscope, and traced through the BATF tracing center. In fact, laboratory separation may be needed in most bombings; the recovery and laboratory procedures are quite simple, however, and can be performed in the field with little equipment and training. Several variations of the basic concept have been tried, some including a polyethylene encapsulant and some including slightly different chemical and physical properties of the individual layers.

### WESTINGHOUSE CERAMIC TAGGANT

The Westinghouse taggant consists of a mixture of rare-earth compounds, bound together into a ceramic-like particle, whose appearance is similar to a grain of sand, and whose largest dimension is approximately 0.2 mm. Each of the rare-earth compounds fluoresces at a characteristic wavelength when illuminated by ultraviolet radiation (325 nanometers). A scanning monochromometer is used to read the wavelength of the various rare-earth compounds, and thus to identify the taggant code. The 10 rare earths that have been evaluated, and their characteristic emission wavelengths are:

Strontium chlorophosphate. europium	447
Yttrium vanadate thulium.	476
Yttrium phosphate cerium, terbium	546
Yttrium vanadate erbium	555
Yttrium vanadate: dysprosium	575
Yttrium vanadate: samarium	608-648
Yttrium vanadate: europium	618
Yttrium oxysulfide europium	626
Strontium fluoroborate. europium,	626
samarium	687
Strontium fluoroborate europium	375

As in the 3M taggant, the Westinghouse taggant incorporates a spotting phosphor which fluoresces in the visible range when illuminated by shortwave ultraviolet radiation (254 nanometers) and magnetic particles, both of which assist in the recovery process. Due to the limited number of rare-earth compounds available, and the fact that the individual components are not ordered like the 3M taggant layers, the library of possible codes is only approximately 3,000, even with three distinct spotting phosphors. Use of different concentrations or pairing of two different taggants to form a unique species can significantly increase the library, with approximately 600,000 codes available for the paired taggant variation. A significant number of compatibility tests have been conducted with the taggant, as have a small number of survivability-recoverability tests. Due to the ceramic nature of the taggant, it is extremely survivable and does not thermally degrade in high-energy explosives (such as boosters), as does the 3M taggant. In addition, since the rare-earth doping is homogeneous throughout the material, the full code can be read from even a small recovered taggant chip. The Westinghouse taggant is extremely gritty, and has been shown to sensitize explosives if not encapsulated in a polyethylene coating.

No additional effort is currently underway with the Westinghouse taggant, due to a Westinghouse concern over liability should some taggant not be fully encapsulated and thus cause sensitization of an explosive material.

From the limited data available, it would appear that the Westinghouse taggant shows interesting potential, particularly due to its high survival rate, although solutions must be sought to ensure 100-percent encapsulation. In addition, some further limitations are imposed by the relatively small code library available and by the rather complex laboratory identification procedure required.

### **CURIE POINT TAGGANT**

The Curie point taggant consists of a collection of five distinct ferrites, packaged with an ultraviolet sensitive spotting phosphor in a binder of potassium silicate. Ferrites exhibit the property that their ferromagnetism disappears when the temperature of the ferrite is raised above a specific temperature, designated the Curie point temperature. Identification of a particular taggant is thus accomplished by placing the recovered taggant in a temperature-controlled chamber and recording the magnetism as a function of temperature. Approximately 50 ferrites have been identified whose Curie point falls in a laboratory practical temperature range. The 50 ferrites, used in combinations of 5 at a time, yield a library of approximately 2 million unique species. As the taggants are ceramics, their survivability in high-energy explosives, such as boosters, should be good. Very preliminary tests have demonstrated the survivability of the taggant in boosters and high-power commercial explosives such as Power Primer. The Curie point taggants share the potential sensitization problem of the Westinghouse taggants, and must therefore be encapsulated with 100-percent certainty. The Curie point taggants have another serious drawback: magnetic separation from powdery materials such as gunpowders and powdery dynamite would be an obvious simple countermeasure.

Electromagnetic taggants incorporated into a detonator, such as the passive harmonic radar taggant investigated by the ATF contractor, Aerospace Corp., offer the possibility of detection at a distance with a relatively low rate of false alarms. All of the concepts so far proposed, however, can be easily defeated by wrapping explosives in metal foil. In addition, inclusion of such devices would probably have a significant effect on the procedures used to manufacture detonators, on detonator cost, and significant false alarms could be caused by common diodes from radios, calculators, and other electronic instruments.

Confinement sharply decreases survival, (of taggants) even under optimum recovery conditions. Only one test has been conducted with explosives confined in a pipe bomb; in that test scores of taggants were recovered from 60 Percent Extra Dynamite. When that result is compared to the chamber survival tests (in which over 1,000 taggants were recovered from 60 Percent Extra) it appears likely that considerably fewer taggants would survive in pipe bomb detonations using one of the more powerful explosives.

Black and smokeless powders are much less energetic than the least energetic dynamite. Gunpowders are normally used as fillers for pipe bombs, however, so the effect of confinement is expected to be considerable. Tests with both black and smokeless powders were conducted in a 20-ft semicircular chamber having steel walls but a sand floor. Due to the poor recovery conditions, only 2 to 3 dozen taggants were recovered for the black powder bombs, and from 0 to 3 for the smokeless powder. When black powder bombs were detonated under near ideal recovery conditions, using the 8' x 12' x 20' bunker, an average of 1,100 taggants survived 1 lb of the FFFg powder. No ideal recovery tests have been conducted with smokeless powders, but the one pipe bomb test with explosives gives an indication that scores to hundreds of taggants should survive.

In summary, the 3M identification taggants survive the detonation of cap-sensitive high explosives in large numbers for small charges which are unconfined. Survival decreases as the charge size increases, but sufficient taggants should survive even a large charge of the most energetic commercial explosive. The effect of confinement significantly reduces taggant survival, but taggants can probably survive pipe bombs filled with low-energy explosives and gunpowder; their survival in pipe bombs filled with higher energy explosives is uncertain. Individual taggants do not survive booster detonation but pellets made from the taggants do. Taggants

would probably survive the explosion of detonators and detonating cord, but there is little or no test data.

Current passenger and carry-on baggage scanning systems at airports have an overall probability of detecting guns or knives of over 80 percent, while they estimate less than a 20-percent detection probability for explosives. (Remember, this is 1980's data)

BATF currently keeps a record of the amount of explosives stolen, recovered, and expended in bombings. While it is possible to trace and allocate cap-sensitive high explosives that are recovered in their original cartridges (by the date-shift code stamped on the cartridge).

The British use a tagging system that apparently consists of different colored threads interspersed in the explosive. The threads do not survive the detonation, but the system cannot be defeated by simply discarding the cartridge, as can the current U.S. date-shift code. The

West Germans use a system similar to the date-shift code, while the Irish dye their explosives (from the single plant) to indicate a destination.

Taggants will be missed quite often if visual recovery means are emphasized.

It appears that the power of the explosive does not significantly affect recovery probability or the laboratory time necessary to separate taggants from the debris. Confinement and the occurrence of fire, however, do significantly affect laboratory recovery time, as the size of the taggants decreases

## **Statement to Congress on ANFO**

Dear Sir:

Referring to questions put to me by Mr. David Garfinkle of Science Applications, Inc. about the initiation and the damage potential of explosive devices loaded with ANFO, I would like to answer you with the following statements.

ANFO generally consists only of ammonium nitrate and fuel oil at a weight ratio of about 95 to 5, but may be used to designate other types of ammonium nitrate based explosives. The density is approximately 0.78 g/cm<sup>3</sup>, the energy density  $E_v = 2.9 \times 10^3 \text{ J/cm}^3$ , and the ratio of specific heats of the gaseous products is  $\gamma = 2.554$ . Under ideal conditions (i.e. quantities of several hundred kg and a strong initiation source) ANFO detonates at a rate of 5 km/s with a Chapman-Jouguet pressure (at the shock front) of 55 kbar. In small samples (e.g. 10 to 20 kg) . even if confined, the detonation velocity is considerably lower, depending on confinement conditions and initiation, and typically between 1.9 and 2.8 km/s. The shock front pressure in these cases is also considerably lower than 55 kbar. Samples with small dimensions and negligible confinement will not detonate at all, (e.g. cylindrical samples in thin plastic confinement 5 cm or less in diameter, or unconfined layers of 5 cm or less in diameter, or unconfined layers of 5 cm or less in thickness) .

The ANFO commercially sold and used in the U.S.A. can generally not be initiated by a detonator only. A "booster" made of about 50 to 500 g of high explosives such as Composition C4, which can be initiated by a detonator only, is generally used to start the detonation. A criminal use of this type ANFO in quantities of 1 or 2 kg does not seem reasonable since the efficiency of a destructive explosive device under these circumstances would generally not be significantly improved beyond that resulting from the booster alone.

It is possible, however, to produce high explosives similar to ANFO which can be detonated by a detonator only. Some ANFO sold and used in the Federal Republic of Germany for mining and quarrying purposes has this property called "cap sensitivity". It is also possible to modify the composition of the blasting agent such that it

becomes cap sensitive, e.g. by replacing the fuel oil by hydrazine hydrate. The sensitivity of ANFO can be increased by certain additives, aluminum powder or potassium perchlorate. In some cases, the sensitivity of the ANFO-like blasting agent can be increased by crushing the ammonium nitrate prills. Most of the premixed ANFO commercially sold in the U.S.A., however, does not become cap sensitive by crushing the prills. ANFO obtained by first crushing prilled ammonium nitrate commercially bought in the U.S.A. and then mixing it with fuel oil will also, in general, not be cap sensitive. If either the ANFO or the ammonium nitrate used to mix it were obtained from certain areas outside the U.S.A., crushing of the prills may render it cap sensitive. In all these cases of "cap sensitivity", however, a high powered detonator (e.g. one containing 1 g base charge) is still needed, and also a certain amount of special information is required, whereas modern propellants as well as all types of black powder can be initiated by a heat source only, like match heads, squibs, or even only an electrically heated wire or a spark.

MATERIAL	REQUIRED FOR INITIATION	
	CONFINED	UNCONFINED
Small amounts of commercial ANFO (-- 2 kg.)	Booster charge of 50-500 g high explosive	(NO Reaction)
Large amounts of commercial ANFO (> 50 ka)	Booster charge of 50-500 g high explosive	Booster charge of 50-500 g high explosive
Sensitized ANFO or special mix blasting agent	Detonator with at least 1g base charge or 6" prima cord (50 grain\ft.) + small detonator like below	Detonator with at least 1 g base charge or 6" prima cord (50 grain\ft.) + small detonator like below
Military explosive like Comp. B or Comp. C-4	Small detonator with about .25 g base charge	Small detonator with about .25 g base charge
Modern propellant or black powder	Heat source like matchhead, squib, hot wire, or spark	(No explosion; only violent burning possible)

To compare the damage producing capability of destructive explosive devices, one has to consider air blast, fragmentation, and potential incendiary effects. Assuming the initiation problems can be resolved for an explosive device containing only a few kg of a blasting agent similar to ANFO, then the air blast caused by this device could do approximately as much air blast damage as a device with the same weight of TNT. The density difference between ANFO and TNT (approximately 0.8 vs. 1.6) would require a larger confinement volume for a device containing ANFO.

Comparing fragmentation of a device loaded with TNT versus one loaded with a blasting agent similar to ANFO, the latter would produce a smaller number of fragments larger in size and with a somewhat lower velocity than the TNT device. The total damage producing capability of the fragments of the ANFO device would probably come fairly close to that of the TNT device. Neither one of the two device types would produce any significant incendiary effect.

The damage producing capability of propellant or black powder loaded devices will generally be significantly

smaller than that of devices loaded with an ANFO-like blasting agent due to the following reasons:

(a) The rate Of energy release is much higher in high explosives, including blasting agents like ANFO, than in propellants including black powder. Expressed, e.g. in Megawatts, a 5 cm diameter device loaded with ANFO delivers energy at a rate of about 10,000 MW; a gun cartridge of the same diameter delivers energy at a rate of about 500 MW.

(b) The rate of detonation of high explosives, including blasting agents like ANFO, is only weakly depending on ambient conditions whereas the propellant burn rate strongly depends on the ambient pressure. Propellants including black powder which are initiated in a metallic shell will frequently violently rupture the shell at a time when only a fraction of the propellant energy has been released, producing only very few medium velocity fragments and only a moderate pressure wave . The burn rate of the still remaining mass of propellant will at the time of the shell rupture drop to a very low rate imposing no other danger than a fire hazard. A high explosive or blasting agent detonated in a metallic confinement like a bomb shell will always produce a number of high velocity fragments and a strong air blast.

To summarize, it can generally be expected that the damage caused with a device loaded with an ANFO-like blasting agent, if it is properly initiated, is somewhat smaller than that of a device of equal weight loaded with TNT, but significantly larger than that of a device of equal weight loaded with black powder or modern propellants.

Very truly yours,  
Roland R. Franzen  
Senior Staff Engineer

*( Thanks Roland! )*

**Thank you for reading our twelfth edition**

**Visit [Resist.com](http://Resist.com) to buy future and archived editions.**

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**

# The PARANOID Newsletter

Proudly reprints the classic military text

## **NIGHT MOVEMENTS**

Translated From The Japanese

by C. Burnett

Night Movements is essential for the study of counter-insurgency and clandestine activities. This rare translation of the original (1913) Japanese military text is generally regarded as the finest study of night fighting ever written. The original manual was used to train snipers, scouts, and saboteurs in World War II. After the war, it became one of the many classic manuals used by insurgents in many parts of the world.

## TRANSLATOR'S PREFACE

The importance of night movements and night attacks in the military operations of the present day is so generally recognized, that any discussion on that point would be more than superfluous. That the Japanese army, from the standpoint of practical experience, is best qualified to discuss such operations, would seem to follow as a matter also beyond discussion. For this reason it occurred to me that the translation of this work of a Japanese officer who was a company commander during the Japanese-Russian War, might, and I venture to say, does contain much that will be of interest and profit to our own service.

Night movements are admittedly among the most difficult operations of war; the margin between victory and defeat is so small that it is a difficult matter to say to just what comparatively trivial reason success or failure may be due. Such being the case, it naturally follows that minute and painstaking training is absolutely necessary if success can be even hoped for. Military writers on this subject have usually recognized that fact, but their treatment of the matter has consisted so largely of vague generalities that they are not of much assistance to Captain Jones in the training of his company and are absolutely useless to Sergeant Smith in leading his squad. This work is not an academic discussion of night movements in general, but is full of valuable practical hints on the training of the small units that go to make up the great military machine; hints not evolved from the inner consciousness, but ideas stamped in the mind by actual experiences of nights on Manchurian battlefields.

Due perhaps to national characteristics, Japanese army training of all kinds proceeds along more exact and minute lines than is usual in our own service. While many may consider that this work errs in that direction, it would be well to consider carefully the necessity for such careful training in the most delicate of all military movements. If Private Brown has not been thoroughly trained and accustomed to night movements, he is sure to make mistakes; multiply him by a hundred or a thousand, and the margin of safety for success will become rather slim, to say the least.

This work has been translated at odd times in the press of much other work of the same general character. For this reason there has been no time to spend on niceties of expression or in polishing up the English; and indeed I am not sure but that following the author's words rather closely does not more than compensate for faulty diction. If the meaning can be comprehended I shall be satisfied and beg indulgence for all the things lacking.

Tokyo, Japan. October, 1913.

This work is uncopyrighted, distribution is unlimited.

**TRAINING IN  
NIGHT MOVEMENTS  
BASED ON  
ACTUAL EXPERIENCES  
IN WAR**

**I. PSYCHOLOGICAL ACTION AT NIGHTTIME.**

From an educational standpoint, a thorough knowledge of psychological processes at night is a most important matter, because the weightiest considerations in night movements are mental ones. Therefore, I will explain this matter at the very beginning.

Having seen a thing with my own eyes, I can form my judgment concerning it; by knowing that there is no danger to my own body, I will be calm. On account of my being calm, there will be no uncertainty; on account of there being no uncertainty, all things, necessarily, will be clear. In order that there may be that clearness, a broad field of view and a clear understanding of facts are necessary. However, at nighttime, a person is not able to see his surroundings; accordingly it is only natural that there should be uncertainty. One cannot know when there will be danger in the darkness just a little ways ahead. In such cases there is a feeling of apprehension, of doubt and uncertainty, and finally there is extremely cautious watchfulness and fear. In short, at nighttime, the mind is agitated and excited.

**Night and Morbid Watchfulness.** -Attention is the term applied to a condition of affairs when the consciousness is concentrated on certain substances or certain ideas. At night, as the field of view is very limited, great attention must be paid to the multitude of surrounding objects; if this is not done, one will quickly fall into danger. In the presence of the enemy, how much more must the amount of watchfulness, on account of its relation to life and death, give rise to the greatest of care-and one becomes unable to distinguish between fact and fancy. As a result of too much care and concentration, what has hitherto been imagination almost ceases to be such, and approaches reality. The imagination is so vivid that unreal things seem real.

**Night and Illusions.**-At night, illusion is easy; there are various kinds of such illusions, as:

1. Confusion which arises from an error of the senses.
2. An illusion which forms a mistaken impression through not having made a proper impression on the senses.
3. An illusion arising entirely from confusion of mind.

At nighttime, illusions very often arise. For example, white clothes hanging on willow trees, or white flags in a cemetery, become ghosts; an old rope in the grass seems a snake; tall pillars, or bundles of Manchurian millet, an enemy, etc.

In the presence of the enemy, such illusions are dangerous.

**At Night, Suggestion is Easy.**-Whenever the mind is agitated, the nerves also become keen. Insignificant causes, also, have the power to suggest things quickly. These suggestions are of various kinds-imitative, inductive, synchronic, etc. On account of such suggestions, confusion, mistakes, false reports, etc., in one detachment, will extend quickly to the entire body. On this account there are not a few examples where a single soldier at nighttime, who fancied that he saw an enemy, quickly gave the whole force the impression that there was, in reality, an enemy present. Again, if one person unexpectedly lays down, or halts, those accompanying him, not understanding the reason for his action, in their uncertainty, do the same. Did not such a thing cause the rout of the Heishi clan at Fushigawa?

At first, probably hearing the noise of a flying bird and thinking it was the enemy, the movement or cry of a single man extended to the whole army. During the Japanese-Russian War, a detachment of the Russian army in a seacoast fortification was thrown into disorder on account of one or two men in front crying out that there was a night attack, thereby causing the whole force to fall into disorder.

**Night Brings out the Weak Points of the Individual.**- A state of uncertainty at night gives rise to the idea of danger; from this there develops a state of fear. Mankind, in crowds, has an excessive mental action. That is, a crowd is conscious of vast power; hence, certain movements, though difficult for the individual, will be bravely carried out by several men together. While one man is fearful and uncertain, a number of men together, will enter into the movement almost without consideration. Therefore, at night, although one man, alone, will be afraid, several together will show no indecision whatever. This fact should be borne in mind in all night movements.

In the matter of mental phenomena, the man who has weak points in the daytime will be spurred on by vanity, love of fame, or perhaps by a self-denying spirit; but when night comes, on account of the lack or the slackness of supervision of his officers and comrades, the individual weakness will quickly show. It is not a good thing to leave the individual without supervision at night, neither is it a good thing to place him in such circumstances as will bring out these weaknesses.

## II.

### IMPORTANT MEASURES WHICH

### CORRECT UNFAVORABLE

### PSYCHOLOGICAL ACTION AT NIGHT.

Although nighttime has the disadvantages mentioned above, there will be times when it will be absolutely necessary to employ soldiers individually. It is, therefore, necessary to train them so that the evils due to fits of characteristic weaknesses will never arise.

**At Night, Especially, Strict Discipline is Necessary.** -Nighttime is the touchstone which determines the value of an army. As supervision is difficult, strict discipline is necessary. The greatest influence of discipline is to repress the weaknesses which grow out of individuality, and to prevent the expression of those weaknesses. An army which does not have good discipline at night, will completely fall to pieces. If the individual is allowed to follow his own desires, an army is ruined. Therefore, successful night operations demand the strictest discipline; it is such discipline that spurs night

success.

**A High Morale and a Firm Offensive Spirit.**-Mental agitation depends upon the state of morale. If the morale be high, there will be no such agitation; therefore, the evils, i. e., the mental phenomena previously described, will not arise. In general, a negative mind always acts unfavorably; therefore, in the case of individuals whose morale is low and who are negative in principle, the following psychological action will arise:

- 1 . A morbid watchfulness.
2. Illusions.
3. Suggestions.
- 4 . Weak points of individual character.

Therefore, a high morale is necessarily required to successfully overcome such weaknesses. As a matter of fact, a high morale is the foundation of successful night operations. A person with a high morale does not stand by passively, but acts, perhaps unconsciously, in a positive manner.

**Silence in Night Movements.** -Silence causes an agitated mind to become cool; on the contrary, disorder causes more confusion. Although, at times, it is both a material and abstract advantage to powerfully excite a man in order to drive him toward a certain objective, the importance of maintaining silence at night, must not be lost sight of. There are, naturally, two reasons for this, viz:

1. In order not to be discovered by the enemy.
2. In order to avoid falling into confusion, yourself.

At night, as it is impossible to discriminate by sight, judgment must be formed from the sounds heard. However, in what way will an ordinary sound which arises in one detachment, be transmitted to others, especially in the case of those detachments who hear this disquieting sound and already believe themselves in danger?

Therefore, at night, in order not to be discovered by the enemy, as well as to prevent falling into disorder, yourself, it is absolutely necessary to remain quiet.

**Night and Massed Formation.**-On account of its large numbers, great things can be accomplished with a massed force; for the self-consciousness of great strength causes great energy. At night, a large massed force destroys those individual characteristics, the various evils of which I have already clearly explained. On account of the difficulty of leadership, communication and contact, confusion and separation are easy. From a psychological standpoint, as well, it is advantageous to avoid the distribution of columns, and to use the close columns instead. A brave, determined advance is of special importance in night movements.

**Night Movements and Self-confidence.**-Self -confidence is the foundation of bravery; it is the requisite of a high morale. If one wishes to obtain self-confidence, there must be no indecision; in order that there may be no indecision, there must be no obscurity. Therefore it follows that conditions should be clearly understood, and that we become rich in experience. That is the reason why thoroughness of reconnaissance, observation, and training are particularly necessary for night movements. If the state of the enemy as well as the terrain be well known, and if the troops be well

trained in night movements, there will be no indecision, and the movement can be carried out by methods and means which may be deemed best. A thing carried out in the belief that success is certain, will be carried out in a recklessly brave manner; that is the reason for the necessity of self confidence at night.

**Night Movements and Self-possession.**-At night, one cannot tell at what distance or at what time there will be personal danger. If the enemy be heard, the danger seems the same whether he be a hundred, or only ten paces away. Therefore, a person of negative spirit feels the enemy pressing upon him, even though in reality, he is far away; and an imaginary enemy becomes the same as a real one. Therefore, in order not to make rash and disorderly movements, causes must be judged coolly.

### III.

#### HOW TO DRESS.

**The Requirements of Dress.**-Dress must conform to the following requirements:

1. Speed.
2. Propriety.
3. Reliability.

To carry out these requirements, training is necessary. It is a bad thing to attach too great weight to speed at first, and make light of propriety and reliability. Therefore, at first, the following requirements must be observed:

1. Do not demand useless rapidity, but rather coolness.
2. Proper arrangement.
3. As far as possible, quietness should be preserved. The necessary things should be taken from their fixed places only when about to be put on, so as to avoid confusion.

**Coolness** - More haste, less speed. If one be confused, he will mistake the proper order or forget important things, and sometimes it will be necessary to change what has already been put on.

**Order** - Order is the shortest road, and if followed, there will be nothing forgotten. However hurried one may be, it is important not to curtail or change the order; therefore, it is necessary to plan carefully, the most suitable order of procedure-a practical impossibility for one without experience. For these reasons, it is a good thing to fix a suitable order of procedure, and carry it out strictly.

**Quietness** - At night, quietness is very necessary, especially in the proximity of the enemy. Therefore, it is important, in time of peace, to demand quietness, and to carry out such a training that there will be no talking or noise. If the soldier has had this training, it is an easy thing to remain quiet. If he has not, it is a very difficult matter. While a sudden demand for quiet is no hardship upon persons accustomed to it, it is most irksome to those who are not so accustomed to it.

**Order of Dressing** - In order that dressing may progress smoothly, a proper order is necessary. In this order, it is important that mind and hand follow natural movements. The following example of correct procedure is from my own

experience:

1. Clothing, shoes and leggings will be worn and put on in the following order: socks, trousers, leggings, blouse, cap.
2. Hang haversack and water bottle over the shoulder.
3. Place the required articles in the knapsack, roll the overcoat; attach tools, spare shoes, and mess tin to the knapsack, and put it on.
4. Take the rifle in the hand (at this time, take off the muzzle cover and place it in its prescribed place).

Although there are times when this order will not be adhered to, and it will be necessary to arrange the clothing so as to take rifle and ammunition first, the habit of handling these articles in their proper order in time of peace is most necessary.

**Peace Time Preparations-Preparedness** - During peace time, weapons, clothing and equipment are naturally arranged in a prescribed place in barracks. Each article should be so arranged that the soldier will put his hand on it naturally, even in the darkness, or in emergencies. On account of the articles being in a fixed place, the soldier often does not realize the advantage of being able to grasp them readily. If the difficulty of searching for obscure articles in the dark be considered, one must realize the great advantage of being able to reach them naturally and easily. Accordingly, while resting on the march, in camp, billet, or bivouac, articles will always be arranged in an orderly manner, so that they may be seized quickly and certainly.

#### IV.

#### TRAINING IN DRESSING.

**Occasions** -This training should be carried out at the same time as the ordinary day training. There are two opportunities for this:

1. At the time of changing the daytime course of training.
2. It can be carried out especially as a drill in dressing.

In the first instance, have the men dress in a fixed place, with each article in a special place. It is important to employ the time so as not to encroach upon time allotted to other drills.

**Orderly Methods** - In the second instance, the following points are important:

1. A comprehension of the method of dressing. While explaining this in barracks, or in a fixed position, give a signal by a whistle, and say: "Now put on such and such a thing." While assistants instruct and inspect the men, teach them the basic principles of what they are doing.
2. Make them dress, unexpectedly, in daytime.

3. Explain the method of dressing at night.
4. Make them dress, unexpectedly, at night.

By such a method of training, the objective may be attained. At this time, without fail, coolness, order and quiet must be maintained. At first, pay no attention to the time consumed; after a little while, demand more speed, and finally have the movement executed at the rate desired.

**Number of Times Practiced** - Whenever an army is accustomed to a certain manner of dressing in its daily life, the dressing is not a difficult matter. On that account, time is not specially allotted for such training but practice will be had whenever there is a good opportunity. However, the following important principles must not be forgotten:

1. To guard against negligence.
2. To review the methods of dressing.

For this reason, it should be practiced every month or so, and whenever the men become careless about it.

## V.

### NIGHT AND VISION.

**Importance of Cultivating the Vision at Night** - At night, one is able to see according to the degree of darkness. The amount of vision also differs naturally and it is important to know the amount under various circumstances. Especially is this true under circumstances where the judgment cannot be formed by hearing, i. e., in rainy weather, or under other noisy conditions, where vision, though insufficient, is superior to hearing. Therefore, the training of the eye at night is a most important matter, as, to a certain degree, it can be strengthened by experience and practice. In the Japanese Russian War, the judgment by sight of soldiers accustomed to the terrain and to night movements, was surprisingly good, and was entirely due to experience.

**Vision at Night Can Be Improved by Training** - One accustomed to night movements, compared to one not so accustomed, is much more able to form correct judgments by sight; for experience sharpens the nerves and increases the faculty of attention. From indications, from methods of comparison, together with other assisting factors, one's judgment soon becomes accurate.

**Night Vision-Detecting and Losing Sight of** - Vision at night differs in degree, also, according to the concentration of attention; in this connection, the following principles are from my own experience:

1. When you follow with your eyes a thing once discovered, you will be able to see it for a long distance.

2. The distance at which you first discover an object, is less than the distance where you lose sight of it. Therefore, at night, when you lose sight of an object you have once discovered, it is difficult to find it a second time. When you follow it with your eye vision is easy, and the distance at which the object is visible becomes much greater, especially if there are supplementary indications. In such a case a thing liable to be unnoticed, will be seen by the observer.

**Night Vision and Objects, and the Color of Surrounding Objects** - The color of the dress has great bearing on vision; and I have learned the following facts from my own observation:

1. On a dark night a white coat can be seen farther than a black one.
2. When there is moonlight, often a black coat can be seen farther than a white one.
3. In any case, a light brown or mouse color can be seen a long distance.
4. A black color against a black background is more difficult to see than white; the latter against white surroundings is more difficult than black.

From these facts, the importance of bearing in mind the color of surrounding objects when fixing the kind of dress, or determining one's movements, is apparent.

**Night Vision and Relations of Light and Shadow** - Night vision differs greatly according to one's position relative to a luminous body and shadow:

1. When a luminous body, such as the moon, is faced, vision is decreased.
2. When the light is behind, vision is increased.
3. When a luminous body is overhead, the mean of increase and decrease is the same.
4. Even though facing the light, if it does not strike the eyes directly, it injures vision but little.
5. One can see when looking from darkness into light, but not when looking from light into darkness.
6. While holding the light yourself, only your own surroundings can be seen.
7. When a light is behind an object, the latter's outlines are clearly visible.
8. A black object or a moving object covered by shadow, is difficult to see.
9. Small objects seem far away, and large ones seem near.
10. Bright objects appear near, and obscure ones far away.

The above facts teach one that, when covered by dark objects, or when moving in the shadow, to look at the bright side from the dark as much as possible, and not have the light directly in front.

## **Relation of the Seasons to Night Vision.**

1. In level, open country, the field of view is extensive.
2. In close country, the opposite is true.

Accordingly, from late in the autumn until the beginning of spring, on account of the grass having withered and the leaves fallen the field of view is extensive. From late in the spring until early autumn on account of the luxuriant grass and trees, the field of view is restricted. During the Manchurian winter (in level country), the field of view is greater than in Japan. In mountainous localities, trees are few, compared to Japan, and the field of view is correspondingly greater.

**Night Vision and our own Posture.**-In looking at objects which have ground objects in their rear, a standing posture is advisable; without such objects in rear, a low posture is best. Therefore, to avoid being seen, take a low posture; if moving, keep physical objects in your rear. Even though such objects be distant, they will be of great assistance.

**Night Vision and Field Glasses.**-Whenever there is light at night from moon or stars, and at twilight and dawn, field glasses will double the power of vision. However, as the glasses narrow the field of view, it is dangerous to depend upon them, except to confirm a thing already seen, or when the locality in which the object to be seen, will appear and move, is fixed.

## VI.

### METHOD OF TRAINING NIGHT VISION.

**General Principles.**-In this training, have the men learn thoroughly the preceding principles. After they have become somewhat experienced, teach them the subject of relative vision under all kinds of circumstances. This will give them a suitable standard of judgment; and it is most necessary that the soldier have various kinds of experiences, so that he may learn how to act when alone.

#### **Important Points of Training --**

1. The execution of movements at night, without reference to the amount of light. In this case, the following training is suggested for the vision:
  - (a) A single soldier moving quietly, first toward the soldier under instruction, and second away from him. The reason for the quiet movement is to prevent any assistance from sound, thus training the soldier in relative vision.
  - (b) A single moving soldier allowing some noise, such as the noise of the bayonet scabbard, water in the canteen, footsteps, etc., first toward the man under instruction, and second a-way from him.
  - (c) A single soldier in different colored clothing, both toward and away from the man under instruction.
  - (d) After a little while, increase the number of soldiers and have them move under the following conditions:
    1. Quietly;
    2. Under ordinary conditions;
    3. With different colored clothing;

4. Toward the one under instruction (discovery), and away from him (losing sight of).  
(e) With a squad under the same conditions as paragraph.

2. Taking the light into consideration.

- (a) With the light (moon, lantern, etc.), above and in the rear.
- (b) With the light at a high place in the front.
- (c) With the light in rear of the object to be seen. (d) When the object to be seen bears the light.
- (e) When the man under instruction bears the light.
- (f) When the object to be seen is on the sky-line, and when not.
- (g) Movements in the shadow.
- (h) The relation between one hidden by an object and one covered by a shadow.

The above practice should be carried out, first, quietly; second, under ordinary conditions; third, with different colored uniforms.

**Methods of Training** - When the number of soldiers under instruction is small, one instructor supervises the instruction in one squad; if the number be large, there will be assistant instructors in charge of each squad. The instruction of all squads will be carried out at the same time, taking care that they be so placed so as not to interfere with each other.

For example, place a squad at A. From this squad send one man (later several men) in the direction B. When he is about to disappear from view, halt him and estimate the distance. Again, based on these principles, send one man (later, several) outside the field of view, in the direction B. with instructions to advance toward A. When he enters the field of view, halt him and estimate the distance.

Try these experiments just mentioned in the following cases and make each man judge distance, etc., for himself, first, quietly; second, under ordinary conditions (singly, several men, squad); third, with different colored uniforms.

**Experiments** - When this kind of training is finished cultivate the understanding and power of judgment by movements at will over various kinds of terrain and under varying conditions of weather, darkness, etc. Teach them to utilize trees, light, terrain, etc., the instructors correcting and criticizing the movements. For example, form the men into a squad, and have other soldiers, from a considerable distance outside the limit of vision, move toward the squad, making use of light, terrain, shadows, etc., as already explained. The squad will watch and criticize the movements, the instructor also adding his criticism. Suitable occasions for teaching the relations of terrain, natural objects, weather, luminous bodies, etc.

## VII.

### HEARING AT NIGHT.

At night, on account of the difficulty of vision, the ears must be trained to listen attentively, and with judgment; the military objective must be attained by a combination of sight and hearing. Even when you cannot approach an object close enough to see it. In many cases, the terrain and the state of the enemy will enable you to accomplish your object by hearing. Again, in many cases, hearing enables one to judge of the proximity of the enemy, and of his movements. Therefore the scope of practical use of hearing at night is very extensive; and it is important that the hearing be well

trained so that one may be able to guess all indications coming from sounds, and at the same time so plan his own movements so as not to furnish the enemy with such indications. On that account, it is necessary to have a criterion by which indications may be judged, and a self-consciousness by which one can regulate his own movements.

### **The Character of the Ground and Sounds.**

1. If the ground be hard, the echo is loud.
2. If the ground be soft, there is but little echo.

That is, if the ground be hard, the noise is sharp; if soft, it is dull.

**Kinds of Covering Substances and Sound** - Noise varies according to the kind of covering substance; therefore it is very necessary to know the relative amount of sound when walking over various kinds of ground.

**The Size of a Detachment and the Relative Weight of Materials** - If a detachment be large, it causes a corresponding amount of noise; and can be heard at a distance; if it be small, the noise is small. If the materials be heavy, the noise carries a great distance, and if they be light, the contrary is true. These relations are coexistent with those of the character of the ground.

### **Weather -**

#### **1. Rain and snow**

- (a) When rain is falling there are great differences in hearing, depending upon the degree of rain.
- (b) When snow is falling, the amount of obstruction to noise, compared to rain, is small. When passing over snow, it varies according to the degree of freezing.

#### **2. Wind**

- (a) When there is no wind, conditions are excellent for hearing, as sound is not at all obstructed.
- (b) When the wind is blowing, conditions are favorable for hearing sounds which occur in the direction from which the wind is blowing, and noises can be heard at a long distance. Opposite conditions produce exactly opposite results.
- (c) Wind blowing in one's ears is disadvantageous, as the noise interferes with hearing.

#### **3. Time of night**

At dead of night, surrounding noises can be heard better than at twilight or dawn.

#### **4. Relation of physical objects**

In level open country, which has no trees, buildings, etc., to interfere with the transmission of sound, noises travel far.

#### **5. Relation of seasons.**

In the winter, not only is the ground frozen, but the leaves of plants, trees, etc., are fallen, the grass is withered and dead, and the crops cut and gathered; therefore, sounds travel especially far.

## VIII

### TRAINING IN HEARING AT NIGHT.

**Important Points to be Considered** - In the following training, have the men understand clearly the relations of the manner of walking, numbers and clothing, to the sound produced; then extend the training as follows:

1. The march of infantry.

- (a) A quiet advance.
- (b) Quick time not in steps (single soldier, several men, squad with and without arms, in different kinds of weather and over different kinds of ground).
- (c) Quick time in step, under same conditions as (b).
- (d) Double time.

2. March of cavalry.

This should be carried out whenever there is a good opportunity, conformable to the above principles.

3. March of artillery.

To be carried out as in (1).

4. The noise of entrenching.

- (a) The noise of digging with a pick.
- (b) The noise of driving a shovel strongly into the ground.
- (c) The noise of pushing a spade into various kinds of ground.
- (d) The noise of a squad carrying on the work freely.

**Methods** - The apportionment of squads according to the number of men, is the same as previously described.

For example, have the necessary number of men advance from the squad at A, in the direction of B. Having faced the squad at A to the rear, have them listen to the noise of entrenching at B; when they can no longer hear it, halt the squad at B, and estimate the distance. Again, have a squad at B, approach the squad at A; when the latter can hear the noise, have them estimate the distance. This training should be carried out with a varying number of men, and under varying conditions of ground and weather. By such means, each man, individually, will learn the proper pace and manner of advance; the noise of working, also, will teach them how to use their tools with a minimum of noise. The following exercises, also, are important: The entrenching of a squad (of so many men) at what distance can it be heard, (a) in quiet weather, (b) when the wind is favorable, (c) when wind is unfavorable, etc.

**Inferences to be drawn from Sound** - To state it briefly, one who is accustomed to noticing sounds at night, is able to form his judgment of the causes by using the various inferences that may be drawn from such sounds. For this reason, such basic instruction is very necessary for soldiers; this instruction, also, will give them a basis for the guidance of

their own movements. For this purpose, it is important to take advantage of every opportunity for instruction in comparing the causes which give rise to the sounds, to the sounds themselves, as for example, the march of a detachment, cavalry, wagons, etc. When well trained in this, the soldier will be able to guess the direction of march, the approximate position with reference to himself, distance, etc. If no good opportunities for such training present themselves, while moving on the many roads, or in their vicinity, listen to all the sounds which arise on the road and practice estimating their causes, direction, distance, etc.

It is very necessary to be able to judge by hearing, the noise of the enemy's artillery entering a position, and the entrenching of infantry. The Japanese-Russian War taught us the necessity of often changing our positions to conform to those of the enemy made during the night; and our only way of determining those movements was from the noise of batteries going into position, entrenching, etc.

## IX.

### QUIET MARCH AT NIGHT.

**Importance** - A quiet march is not only important for the purpose of taking the enemy unawares, but, at the same time, it prevents confusion in our own ranks. A quiet night march demands absolute silence and a suitable pace. In the Japanese-Russian War, although it was difficult for large bodies to move without the noise of marching, the advantage of quiet movements was indisputably shown. There are many cases in which an absolutely quiet march is demanded of individuals, such as patrols, outposts, etc.; such training should be borne in mind when these men become units of a larger force.

#### **Important Cautions in a Night March.**

##### 1. Care as to clothing.

It is important that there be no noise from the clothing and equipments; this should be true at double time as well as at quick time. To carry this into effect, the following points must be especially borne in mind:

- (a) That there shall be no noise from the ammunition in the ammunition boxes.
- (b) That no noise arises from the movements of the bayonet scabbard.
- (c) The belt must be kept tight without fail.
- (d) That the contents of the haversack make no noise.
- (e) When the overcoat is worn, the skirt must be fastened up.

##### 2. Individual precautions.

- (a) When coughing cannot be prevented, cover the mouth with the coat sleeve.
- (b) Be careful to hold the rifle so that it will not strike the ground.
- (c) See that no noise arises from the rifle sling and swivel.

### 3. A detachment.

- (a) Each soldier will take care not to bump into his neighbor.
- (b) There will be no talking between adjacent files.
- (c) Each soldier will take care not to make it necessary to leave ranks (for lost clothing, equipment, etc.).

### 4. Manner of walking.

- (a) In short grass, raise the feet high.
- (b) In long grass, keep the feet low.
- (c) In climbing a hill, plant the toe first.
- (d) In descending a hill, plant the heel first.
- (e) Don't stumble or fall down.

### 5. Connection.

- (a) In-line, conform to the movements of the soldier on the right or left; in column, on the soldier in front.
- (b) Don't hang the head; if this is done, connection will surely be lost.
- (c) Don't leave ranks, or halt unnecessarily.
- (d) At a halt, close up, but do not bump against the man in front.
- (e) Listen to signals, commands, etc., and be sure not to mistake them.

## X.

### TRAINING IN QUIET MARCHES AT NIGHT.

**Dress** - At first, the training should be without arms, proceeding step by step until fully armed and equipped. During this time, the men must study how to prevent any noise arising from any part of their dress or equipment.

**Order of Training** - General explanations will be made to the men on the ground where the quiet night march is to be made. After indicating the manner of walking, each soldier will be made to practice it under the supervision of an officer, who will explain the principles involved. When these principles have been understood, the number of men will be gradually increased, and the principles of the quiet march, individually, and by squad, will be taught.

**Method of Carrying Out the Above Training** - This training will be carried out at the same time and with the same formations as the training for hearing.

**Cautions** - Although a quiet night march is very important, it must not be allowed to injure the offensive spirit. A quiet movement never means a spiritless one, and it must be made clearly evident that minute care never means hesitation. In a quiet night march all noise will be prohibited, and each man must take care not to cause confusion to the entire command by his individual mistakes and errors.

## XI.

### THE CROSSING OF ROUGH GROUND AT NIGHT.

**Importance of Practice** - At night, the different ground objects differ in aspect from the daytime. Objects, which in the day are no great obstacle, become formidable at night. Open level country which can be easily crossed at night, cannot be expected in practice; accordingly, the crossing of rough ground, orderly, quickly and exactly, without confusion and without delay, is a very important thing for an army. If proper training be had, such a movement is not very difficult; training insures a minimum of fatigue and disorder.

#### **Summary -**

1. As falling down often follows a stumble, care must be taken not to stumble. Even after stumbling, one is not liable to fall down unless leaning forward; therefore, that tendency must be avoided.
2. As falling down is sometimes unavoidable, the following precautions must not be neglected:
  - (a) Arrange clothing, equipment, etc., so that there will be nothing lost or broken; special care must be taken not to lose the hat.
  - (b) Not to drop or break the rifle.
  - (c) Not to talk or make any noise.
3. The method of carrying the rifle varies with the ground and ground objects; in a forest, etc., it is a good thing to carry it in the hand, taking proper care not to cause any danger to the rank in front.
4. If, while in a squad, the soldier only pays attention to what is underneath his feet, the following disadvantages must occur:
  - (a) The march will be delayed.
  - (b) Collision in front and rear.
  - (c) Loss of connection.
5. When obstacles are encountered, they will be passed in accordance with the principles laid down under that subject.

## XII.

### TRAINING IN CROSSING

### ROUGH GROUND AT NIGHT.

**Clothing** - In these movements, care in the matter of dress is especially important. If untrained men are made to carry arms from the very first, not only will the rifles get broken, but the men will sustain personal injuries as well.

Therefore, if practicable, dummy guns should be substituted for the service rifles in the early stages of the training; this training should be carried out in the following order:

- (a) Without arms.
- (b) With dummy rifles.
- (c) With service rifles.
- (d) With full equipment.

### **Order of Training -**

1. At the very first, the training should be individual, allowing an abundance of time for the execution of the movement; at this time the principles should be thoroughly inculcated.
2. Proceed, in a short time, by squad; at first, from column of fours in single rank extending to double and quadruple ranks, and in line as well. At times, have a simple change of direction or formation executed. The change of direction by squad to the right or left is simple, and will be of practical use; it is important, also, to teach, practically, such important movements as the change of formation from column to line, line to column, company column to line, etc.
3. When well trained in these movements, require them to be made silently. Even though the passage of uneven ground is a difficult matter, repeated practice makes it comparatively easy. During the Japanese Russian War, the greater part of those who fell down during such movements were newly arrived reservists.

## XIII.

### DETERMINATION OF DIRECTION AT NIGHT.

**Its Importance** - That the determination of direction, day or night, is important, is clearly evident. Especially at night, it is easy to mistake directions, and it is difficult to discover the mistake quickly. If the direction is once mistaken, the execution of one's mission is practically impossible; therefore, the quick determination of direction, at any time, is a most important matter.

### **Methods of Determining Direction - By fixed Stars:**

1. Direction can be determined by the position of the greater number of fixed stars, especially by the north star. Accordingly, on a clear night, the direction can be accurately fixed by this star. The north star is a fixed star in the tail of the Little Bear constellation. It is on the prolongation of the line b-a, which connects two stars of the Great Bear constellation, and at about

five times the distance between these two stars. On one flank of the Little Bear constellation, which is opposite the Great Bear, is a collection of stars in the shape of a cross, called Anteus.\* Anteus always moves, maintaining this relation with the north star at the center. Therefore, when these stars are seen, the recognition of the north star is easy, and the north can be fixed.

\*The constellation shown in the cut and noted in the text as "Anteus" is the well known one of "Cassiopeia." It is in the form of an irregular letter "W" instead of being in the shape of a cross as stated above.-Translator.

## 2. Method by the moon.

Although it is difficult to determine direction by the position of the moon, the latter has the advantage of being recognizable even on nights when all the stars cannot be seen. The moon crosses the meridian about noon on the first lunar day, and it moves about fifty minutes behind the sun every day. Therefore, if the age of the moon be known, the approximate passing of the meridian can be easily computed. Its approximate age can be computed from the shape of its bright portion.

## 3. Method by a map.

A map indicates directions in a general way, by its outlines. Either the upper portion is north, or the direction is indicated. Therefore, if the map can be oriented upon the actual ground, direction can be easily determined. Even though such an orientation is difficult at night, the general directions can be fixed from memory, or from the direction of roads, mountains or rivers. If there be a compass it can be done simply and conveniently.

## 4. Method by compass.

The blue end of the needle generally indicates the north. In a dense fog, snow storm, or in the darkness within a forest, in all cases when a mark is difficult to see, there is no way as certain as the compass.

## 5. Other methods.

The condition of trees, the position of the windows in houses in cold countries, the direction of prevailing winds of a locality, the position of wind shelters, wind mills, etc., all aid in determining direction.

# XIV.

## TRAINING IN DETERMINING DIRECTION.

**How to Find the North Star and How to Use it** - In locating the north star, the instructor first points it out to each soldier. Next, he explains its relations to the previously described constellations. At another time, he will take the same men away from barracks, and have them individually, locate the star. Practice will soon enable them to look up and discover it quickly. When once discovered, it fixes the north, and the other directions easily follow. Next, using this star as a guide, order the men to move in any required direction, by such commands, as: "Move southeast; northwest; etc. " When they can do this accurately, they have learned how to use the star.

**Method by Looking at the Compass** - When examining a compass, except on a moonlight night, a light must be made, and each soldier requires practice on that point.

## XV.

### METHOD OF MAKING A LIGHT AT NIGHT.

**Its Importance** - In any case, it is important that the light should not be visible to the enemy, either directly or from its reflection on trees, etc.; therefore, the following principles must be observed:

- (a) That the light does not leak out directly.
- (b) That it is not reflected by any object.

**Manner of Making a Light** - From the preceding principles, we see that the proper way to make a light, is to take advantage of the configuration of the ground, the various physical objects, etc. The following are examples:

1. If there are any trees in the vicinity, make the light behind them using the body also to shelter it.
2. Use embankments, houses, stone walls, etc., in the same way.
3. When there are no such covering objects, proceed as follows:
  - (a) Two men clasp arms together, their backs toward the enemy; using their bodies as a shelter, hold the cap near the ground, and make a light in the cap.
  - (b) Use the cape of the overcoat as a shelter for the light.
  - (c) One man alone, will squat down on the ground, and make a light between his legs, the ground, and the upper part of his body.
  - (d) Light the tobacco (Japanese), in the pipe quickly; blow it, and examine the object (watch compass, etc.) -

**Individual Training** - After the above basic methods are understood, each man will be made to carry matches, and lights will be made singly or in groups, and then inspected. For example, have the men under instruction advance the necessary distance in front of the squad A; at that place, have them make a light so that it will not be visible from A. If a light be seen, have the one who made it do it over and instruct him carefully.

**This Method is a Common Sense One** - As this method is a common sense one, much instruction will not be necessary. It will be sufficient, to test the memory at times. Thoughtful soldiers will do this, properly, even without instruction.

## XVI.

### CONNECTION AND CONNECTING

#### FILES AT NIGHT.

#### **Methods**

##### I. Method by sound.

On a dark night, a luminous medium is necessary in maintaining connection by sight. Accordingly, when conditions

forbid the use of a light, sound must be depended upon and preconcerted signals are required. For example:

- (a) Sound made by striking the rifle butt.
- (b) Use of the whistle.
- (c) In addition, various methods suitable to the conditions.

When such signals become complicated, their usefulness is destroyed; they must therefore, be very simple. For example:

- (a) Signal for attention.
- (b) Signal for announcing one's position.
- (c) Signal when the enemy, or something suspicious is discovered.
- (d) Signals for advance, retreat, summoning, etc.

These signals may be fixed by the tone of the whistle, or by the number of blows struck on the rifle butt. In this instruction, have the assistant instructors, at first, give these signals to the recruits; and then have the signals agreed upon carried out within the squad of recruits under the supervision of the instructors.

## 2. Method of connection by signals.

Methods of communication on a large scale by revolving or flashing lights, etc., are very important, but we shall only discuss the simpler methods here.

- (a) Beacon lights.
- (b) Matches.
- (c) Match-cord.
- (d) Bull's-eye lantern.
- (e) White cloth.

During the Japanese-Russian War, beacon lights were frequently used, especially by the Russians. Lanterns, straw, or some combustible material was tied on the end of poles, which were erected at necessary places (oil was used if there was any on hand). On account of the nature of the work, it was usually performed by officers, as it was found dangerous to entrust it to enlisted men.

Matches cannot be used for connection, except in the very simplest cases. For example, they can only be used for the advance or retreat of patrols, or for the transmission of very important single signals.

By a rope match, comparatively many signals can be transmitted, as for example:

- (a) The round one has a certain meaning.
- (b) The flat one has a certain meaning.
- (c) The vertical one has a certain meaning.

In addition, by various complicated vibrations, many different signals can be transmitted. The distances at which this rope match is visible are fixed by experiments, and each soldier must be taught the effective distance.

Dark lanterns can be used at short distances in flashing messages. Though the distance of transmission varies with the strength of the flame, it can, under many conditions, reach a comparatively great distance. When accustomed to this method of transmission, it will be found very convenient for outpost duty, and it has the further advantage of being concealed from the enemy. During the Japanese-Russian War, the author made one Out of an empty vegetable can. Each squad was supplied with one of these cans, and they proved of great value.

## 3. Connecting files.

Even though the movement of connecting files at night are similar to those in the day time, the amount of difficulty varies greatly. Accordingly, training under varying conditions is necessary. The terrain, state of the roads, conditions of the hour, etc., have a great influence. This work must be carried out accurately in the following directions:

- (a) In a longitudinal direction, at a halt and when connecting moving bodies.
- (b) In a horizontal direction under similar conditions.

#### 4. Messengers.

The proper performance of the duties of night messengers is very difficult, because at night time, on account of losing directions, mistaking roads, together with the mental state of doubt and fear of the messenger, there are many times when their movement is stopped, or their objective not carried out. The progress in the use of the telephone, telegraph, and other methods of transmission, has not rendered the training of messengers useless.

#### 5. Methods by which messengers may advance.

- (a) By roads.
- (b) By rushes, from object to object.
- (c) Moving along a prominent extended physical object (as river, mountain, forest, etc.).
- (d) In a certain fixed direction (by compass, etc.).
- (e) By a mark, light, etc.,

The method by roads is very safe if the roads are prominent, and there is no danger of losing the way. Such roads as those of China which connect village with village, are very uncertain and it was very easy to get lost. When traveling on a road, the following precautions are important:

1. Care and discrimination in the forks of a road.
2. Marks or signs at important places.
3. Pay attention to physical objects on the road, or at the side of the road.
4. Other unusual relations.
5. The relation between the gradual change in the direction of a road and the forks of a road.
6. The manner in which a road enters or leaves a village.

For example, in sending an orderly from B to A, give him directions about the road he is to follow, in this manner: "Move from B toward A; at the three forks in the road near an umbrella shaped pine tree, take the right road; after crossing a bridge, you will hear the noise of a water-wheel; continuing on this road, you will see a village on the left, - which you will be able to pick out from its fire-tower, and A is but about five minutes walk beyond, etc."

The method of advancing by rushes from object to object, was used in crossing the Manchurian rice fields in winter, and in crossing ground where there were no roads. Such conditions forced us to adopt the above method.

#### 7. Cautions respecting the above method:

- (a) After entering the physical object (woods, etc.), do not mistake the direction on exit.
- (b) If possible to pass around the flank of the object, it is preferable to going through it.
- (c) The interior of villages and woods are important, but it is best not to enter them, except when clearly advantageous to do so; roads in the interior of a village are complicated, and it is often easy to lose direction.

When there is no map, memorize beforehand the names of the villages in order, as it will facilitate communication

with the inhabitants of those villages. When advancing in an unknown country, you will be able to take proper road to the next village even though the natives could not tell you the road to the destination of the day's march. Whenever there are no natives, or you cannot communicate with them, it is difficult to advance without a map. In such cases, objects or marks previously noted in the daytime must be depended upon, but it is a most difficult matter, at best.

8. Method by moving along a prominent extended object (river, woods, etc.).

For example, in going from A to B, when the road is indistinct and cannot be used, follow along the stream which flows in the direction A-B. In important cases, the messenger will go down to the stream to verify the road.

By this method, or by the direction of mountain ranges, rice-fields, ravines, etc., the general direction can be kept, but great obstacles will frequently be encountered, which only determination and boldness will conquer.

9. A messenger's looking forward and backward, and memory.

A messenger must always pay attention to the following things with reference to the road traversed, or physical objects passed on the way:

(a) Look back at the physical objects which he passes and at other things which will serve as marks, committing them all to memory.

(b) Memorize physical objects which are at important points (so that he will be able to recognize those points upon arrival there).

(c) In the daytime, think of the night; memorize the marks, and at the same time, judge how the shadows will appear at night. (Remember that projecting trees will not be visible at night, as they will be covered by objects in rear.)

(d) Establish special recognizing marks, as:

1. White cloth., white paper, etc., in branches of trees.

2. Special guiding trees.

3. Scatter paper, white powder, or other easily recognizable substances along the road.

### **Cautions for all Connecting Files.**

(a) Avoid the double time for connecting purposes. It is not only noisy, but there is the danger of falling down as well.

(b) The amount of sound required when reporting and for connection purposes will vary according to the conditions which obtain at the time.

(c) Connecting files of a column, upon arriving at a fork in the road, must not lose touch with the column~in rear or lose sight of the detachment in front. At such times, paper or white powder will be scattered (See chapter relating to night marches).

(d) The position of connecting files should be such that they can see our own forces, and be seen by them.

(e) They must make the transmission of messages quick and certain.

10. Method by relays.

(a) Long distance relays-written and verbal messages.

(b) Short relays-written and verbal messages.

The method by relays is frequently carried out in war time, and it is therefore necessary that all soldiers be well trained in this work. In the training for long distance relays, it is very important to begin with very simple methods, gradually working up to difficult conditions.

For example, place soldiers as indicated above; from the position of the instructor at A, give verbal orders and messages to No. 1 in the vicinity of the instructor, and cause the message to be transmitted to Nos. 2, 3, etc., to the last post, who transmits it to the instructor. This exercise can be carried out during other drills, or while on the march.

In short relays, also, it will be found profitable to begin the training as described above. Whenever necessary, the message will be transmitted in a low tone from one soldier to another. Practice may be carried out during night maneuvers, or on the march.

## XVII.

### NIGHT FIRING.

Night firing must not be carried out unnecessarily; however, if conditions are such that it can be carried out accurately and without danger, it is permissible. Night firing by squad is most effective in volley firing by command; but it is important that training in individual fire, also, be carried out, as that kind of firing must be used at point blank ranges.

#### **Cautions for Individuals when Firing.**

1. At night, keep cool and obey the commands of your leader.
2. Night firing is usually too high; therefore, take care not to incline the upper part of the body to the rear, or raise the muzzle of the rifle above the horizontal.
3. In firing at night, it is a good thing to release the trigger by one pressure of the finger, instead of the usual method.
4. Never get excited after firing; keep cool.
5. When firing is stopped, turn the safety without fail.

## XVIII.

### TRAINING IN NIGHT FIRING.

**Horizontal Firing and Posture** -The kneeling position is most suitable for horizontal firing; when aiming, raise the buttock from the right heel and hold the rifle as in the standing position. This method of aiming is suitable to all kinds of terrain, and can be done in double rank as well as in single rank.

**Method and Order of Training** - This training may be carried out as follows:

- (a) Train each soldier to hold his rifle horizontally.
- (b) By such training he will soon be able to hold it so, naturally.

1. Formation.

The following points are essential:

- (a) One soldier must not interfere with another.
- (b) It must be convenient for supervision by an officer.

In line with one pace interval fulfills both these requirements. This drill trains the muscles to work involuntarily; and daytime will be found most convenient for training and supervision.

2. Opportunity for training.

Daytime is best for this training, on account of its convenience for observation and instruction.

3. Methods.

Have each soldier close his eyes and level his rifle, according to the principles that have been explained to him. After the rifle has been brought against the cheek, the soldier will open his eyes and examine it. Next have this movement executed by squad by command, just as in pointing and aiming drill. When this movement is well understood, order the men to close their eyes, and, while in that condition, put up a target and have them carry out horizontal fire against it.

## XIX.

### NIGHT BAYONET EXERCISES.

**Importance of Such Drill** - A night battle is a hand to hand fight in which the bayonet must be used; therefore, the bayonet is the one cause of success in night attacks. When well trained in such fighting, it raises self-confidence, increases bravery, and drives away fear.

#### **Cautions in the Use of the Bayonet at Night.**

1. At night, on account of an excessive watchfulness there is a tendency to misjudge the proximity of the enemy, and to dash upon him with the determination to overthrow him with the body alone, without making use of the bayonet.
2. Make the men understand that they can overthrow the enemy only after they have first put away all thought of their own lives.

3. At the time of the attack and charge, it is important not to stumble and fall; in order to avoid this, care must be exercised in placing the feet on the ground.
4. Care will be exercised in the dress, and in the handling of dummy guns, etc.
5. An accurate and rigid posture is necessary in executing this movement in the prescribed manner
6. During training, the following points will be observed:
  - (a) Be cool, and do not make any sound without permission.
  - (b) High morale and overflowing spirits are necessary.
  - (c) Cultivate an aggressive spirit.

## XX.

### TRAINING IN NIGHT BAYONET FENCING.

**Scope of Training** - In night training in bayonet fencing, it will not be necessary to carry out all the movements given in the Fencing Manual, because at nighttime, it is important to overthrow the enemy in the first charge by a vigorous and violent offensive, in which skillful dexterity is no great necessity. Therefore, the following training will be found sufficient:

- (a) Direct thrust against temporary targets.
- (b) Fundamental drill.

When these two things are taught sufficiently, the requirements of a night bayonet attack can be fulfilled.

#### **Method of Training.**

1. Against dummy figures.

Each soldier will be made to charge against a hypothetical enemy (as used in Russia), or against a white cloth, or figure of a man carried by the instructor. At first the figure will be in a fixed position, but later, the soldier will charge seeking the target and not knowing its position beforehand. As the training progresses, make surprise targets of white cloth, dummy figures, targets, etc., and at suitable times, have them appear suddenly before the soldier.

2. Fundamental training.

In this training, the instructor-Non-commissioned officer, or First Class Private-wears defensive armor, and if necessary, face armor as well. The soldiers under instruction wear fencing gloves only, or the regulation clothing. The instructor calls out a name, and the soldier charges several times, being relieved in turn. At this time the soldier must be taught not to fear the instructor's bayonet, but he must be made to approach very close to the instructor. Try to make the exercise as realistic as possible. On moonlight nights, this exercise will conform to that of the daytime, but the best way to take advantage of the light can be studied.

## XXI.

### NIGHT ENTRENCHING.

**Importance** - The construction of fortifications, on the offensive or defensive, in the day or night, is a most important matter. Even though prevented in daytime by the pressure of battle, the night will bring an opportunity for entrenching. Accordingly it follows, that, in many cases in actual warfare, entrenchments are constructed in front of the enemy at night. For this reason training in night entrenching is most necessary. While such work is comparatively easy on a moonlight night, it is a very difficult thing on a dark night.

#### **Night entrenching and Important Point in Training.**

1. Each man marks out his own section, and begins digging from close by his feet.
2. Care will be taken to connect the individual excavations.
3. It is easy to make the trench too narrow; therefore caution is enjoined in this respect.
4. Be careful that the excavated earth is not thrown too far or too near; each man will watch the way he throws the dirt and apply his strength accordingly.
5. In using the shovel and the spade, much noise is caused if the dirt be allowed to fall from an unnecessary height; therefore the strength should be applied when the shovel is near the ground.
6. Each man's section should be large enough to prevent his being struck by his neighbor's tools.
7. If discovered by the enemy's search lights, do not become confused; simply lie down.
8. If attacked by the enemy, do not throw the tools away; either put them in the place where the rifles were left, or in some other fixed position.
9. Do not use the pick unless necessary, as this tool requires a wide frontage.
10. Do not scrape tools together in order to clean off the dirt; use a chip of wood or the toe of the shoe.
11. Cautions regarding reliefs:
  - (a) At the time of relief, entrenching tools will be handed to the relief without any talking.
  - (b) Care will be taken that no vacant spaces are left between the workmen.
  - (c) The working place should not be left, except upon arrival of the relief. Each man will carry his rifle.
  - (d) Whenever unavoidable, leave the tools sticking up in the ground where they can be easily found. In order to prevent losing them, it is a good thing to tie a piece of cloth on the handle.

## XXII.

### TRAINING IN NIGHT ENTRENCHING.

**Methods.-** To carry out this training, march the squad on a dark night, to the training ground. First, have the men dig individually, and explain to them how it differs from the work in the daytime. Next, place two or more men side by side, indicate each one's sector, and have each one execute his prescribed portion. If possible to do so, it will be found advantageous for the men to see, in the day, the result of their night labors. At this time, too, they must be taught the differences in sound resulting from the differences in the character of ground and the tools used.

**Cautions.-** In this training, the following points should be especially noted:

1. At nighttime, do not have idle soldiers looking on at the work.
2. Take only a small squad at a time, as it is impossible to oversee, properly, the work of a large number.
3. In addition to their own work, have the men listen to the noise of others working, thus cultivating their judgment as to distance, number of men working, etc.
4. Don't limit the work to nighttime only. Make the men understand what is required by work in rainy and snowy weather, when such work is difficult.
5. Carry out this work as often as possible, so that they will become accustomed to it.

Method by Using Sand Bags.-(See detachment entrenching).

## XXIII.

### METHODS OF RECOGNIZING

### FRIENDLY TROOPS AT NIGHT.

**Importance.-** At night time there is danger of attacking and fighting our own forces; accordingly the quick recognition of our own troops is most important. If that recognition be delayed, there will be the great danger of losing the initiative.

## Methods of Recognition.

### 1. Speech.

- (a) Different words from those in daily use.
- (b) Countersign.

### 2. Uniform.

- (a) Different from that in daily use.
- (b) Special distinguishing marks.

Words and clothing in daily use are not sufficient to rely upon in war time. During the Japanese Russian War, the Russians frequently wore our uniform, or Chinese clothing, and used our speech.

**Disadvantages of Speech.-** At night, the one who speaks first, is at a disadvantage. In the old days of sword and spear fighting, there was no particular danger in speech, unless very close together; but today, one who is believed to be an enemy, is quickly killed by firearms.

**Suitable Methods of Recognition.-** As stated above when there is a difference of language and uniform, that is a suitable method for quick recognition; but it is most important to gain the initiative. In order to prevent the enemy from gaining the initiative, such methods as striking the rifle stock, signals by whistle, etc., may be used, these methods being applicable to any country. However, on a very dark night, especially in a confused bayonet fight, such methods are not sufficient; accordingly, the men must wear some special distinguishing\* mark, which can be readily identified. In this case the distinguishing marks must be recognizable along the whole front, and, if possible, should be worn so as not to be visible to the enemy.

## XXIV.

### NIGHT DEMOLITION WORK.

**Training.-** When a position for assaulting is taken, the position of the enemy must be reconnoitered. Having made certain of the presence of obstacles in front of the enemy and their position and character, they must be destroyed before the charge. Engineer troops are most suitable for this work, but infantry, as well, must be able to open their own road. This demolition is a very difficult matter, especially in the case of independent infantry, not supplied with explosives. Therefore thorough training in peace time is most necessary.

#### Requisites for Demolition Work.

- (a) Brave men who do not fear death.
- (b) Quick, clever men.
- (c) Cool men.

Even though possessed of the above characteristics, if they do not take advantage of a good opportunity, success is uncertain. It is the duty of officers to watch for good opportunities.

**Important Principles of Demolition Work.** - Of course the point to be demolished must conform to the tactical requirements, and must be such a place that, having been broken, troops can enter instantly. The space demolished should be wide enough for a column of fours to pass through. Sufficient preparation should be made for this demolition, and its execution must be rapid. The obstacle should be approached, as far as possible, without the knowledge of the enemy; when this is impossible, it must be demolished under the protection of friendly troops. Several places should be selected for demolition so that there will be a good prospect of success somewhere.

**Methods of Training.**- This work is engineering work, and the men should be trained in it first in the daytime. After they thoroughly understand its requirements, the work will be carried on at night. While of course it is desirable that all men should have this training, on account of its difficult nature, it will be found sufficient to train only a selected number.

## XXV.

### METHODS OF USING

#### HAND GRENADES AT NIGHT.

Hand grenades have become more important than ever on account of their practical use in the Japanese Russian War; in future wars, their use will become more and more general. Even though there will be but few instances where great training will be required in their use, if they are not used properly success is impossible and they will only serve to alarm the enemy. Therefore each soldier will be trained in their use, at least to the extent of becoming brave enough to carry them without hesitation. On account of their danger, soldiers will first be accustomed to them in the daytime; then later, at nighttime, they will throw them at targets made of lanterns or lights. Whenever there are but few hand grenades, small packages of the same weight will be constructed; to these will be attached the same weight of throwing rope, and thus the effort necessary for throwing the grenades can be ascertained. Soldiers will thus learn the amount of effort necessary for various distances. The hurling of hand grenades is the prelude of the charge; if the charge comes too long after the shock of the grenades, success is most uncertain; the enemy's works must be penetrated immediately after the hand grenades are thrown.

## XXVI.

### NIGHT SENTINELS.

**Training.** - Sentinels will be trained in the daytime as well as at night. At night, he must be able to move under any condition that may arise during that time. This training should be begun only after the soldier understands clearly the essential points of the relations between sound and vision, the determination of direction, silent night marches etc.

**Night, and Position of Sentinels.-** (See chapter on sight and hearing).

Even though possessed of the above characteristics, if they do not take advantage of a good opportunity, success is uncertain. It is the duty of officers to watch for good opportunities.

1. A position with a broad field of view.
2. A position with no obstruction to the field of view.
3. A position where hearing is not interfered with.
4. A position not visible to the enemy, but convenient for our own view. For example:
  - (a) To keep open ground in front.
  - (b) To avoid a windy locality, or one where there are water-wheels, etc.
  - (c) At night, to be in the shadow of a tree with the moonlight behind.
  - (d) A position from which the sky-line is visible is advantageous, even on a dark night.
  - (e) A position where you can be seen a long distance against the sky-line, is disadvantageous.
  - (f) A position which is known to the natives is disadvantageous.
  - (g) To be always in a fixed position is disadvantageous.
  - (h) Terrain which prevents the enemy from attacking suddenly is advantageous.

Along the Shaho river in Manchuria, a sentinel in a fixed position was frequently surprised by the enemy, and there were many instances of such surprise caused by the fact that the natives knew the sentinel's position.

When in the daytime position at A, the sentinel can see well in the enemy's direction, but at night, such a position can be easily seen by the enemy; therefore the sentinel's post should be changed to B, from which place an enemy appearing at A can be easily discovered. The sentinel's position should be chosen from the most suitable ones in the vicinity, and the sentinel, himself, should improve his post in accordance with previously mentioned requirements. To stand carelessly with the rifle in the hand, naturally invites danger. This caution is especially important to men on such duties as sentinel on outpost, etc., which is the first line of defense of an army at the halt.

**Night Sentinels and Posture.-** The posture of sentinels will be laid down in instructions. In fixing the posture, the relation of the ground and physical objects must be borne in mind. At night, the following points will be especially noted:

- (a) The posture should be lower than objects which are in rear.
- (b) Avoid a posture visible on the sky-line.
- (c) Other points are the same as in daytime.

**Night Sentinels and Reconnaissance.-** The principles of night reconnaissance depend upon the following points:

- (a) Follow along physical objects as much as possible, keeping the body low, and holding the breath; you will thus be able to hear any noise.
- (b) Try to see objects on the sky-line.
- (c) Bear in mind the relation between physical objects (trees, etc.) and the moon; take care that there is no enemy concealed in the shadow.
- (d) Form your judgment of conditions from the sounds heard.
- (e) Don't move unnecessarily.

**A Sentinel's Challenge at Night.-** Our preparation at night must be in accordance with the movements of the enemy. Signals, countersigns, etc., will not be used unnecessarily. It is important that we should know, first, something about the enemy. At this time, the sentinel's posture will be in accordance with the following requirements:

- (a) When able to fire make preparations for so doing; if fired at by the enemy, take such a posture that you will not be hit, i. e., lie down.
- (b) When there is no other course than the use of the bayonet, try to overthrow the enemy by one blow; care should be taken not to be surprised.

In short, challenge quickly, and do not allow the enemy to obtain the initiative.

**Night Sentinels and Firing.-** Sentinels should be careful about firing, even in the daytime; how much more is this true at night! Such firing must conform to the following conditions:

- (a) When danger is pressing, and there is no time to return with a report.
- (b) Whenever necessary for the sentinel's own safety.
- (c) Whenever certain of hitting the enemy's patrols, etc.
- (d) Whenever the enemy's returning patrol already knows the sentinel's position, and the latter is able to fire effectively.

We have already explained why sentinels should not fire unnecessarily at night. From experiences in actual warfare, it has been found that when a sentinel remains silent at his post, he gradually becomes excited, and fear and illusions fill his mind. Trees seem enemies, and naturally, firing soon follows.

During the Japanese-Russian War, when in contact with the enemy, the latter frequently attacked our sentinels in the following manner:

For example, some of the enemy's patrols about dusk, persistently operated in the direction B. Even at night they did not leave, but gradually approached closer in the darkness, just as if they were going to charge our post, and finally opened fire. Our sentinels, being diverted by this, returned the fire. The enemy's detachment at C, locating the post by the flash and noise of firing, charged suddenly from C.

Sentinels confronting the enemy are in practically the same situation as in fortress warfare. Vigilance, of course, should be stricter than on the march; but there are many examples which show that the sentinel's firing guides the enemy and enables him to approach closely.

**Night Sentinels and Reports.-** Night sentinels, when making reports, will pay special attention to the following points:

- (a) At the time of moving not to make any noise or cast any shadows.
- (b) Not to move at the double time unless absolutely necessary, nor make any noise.
- (c) The report will be made in a low voice, just mutually audible.
- (d) At the time of the report (made to visiting patrols or others), not to let the enemy take advantage of it, or, if the enemy knows that one man has gone back to the rear to report, not to allow that fact to be taken advantage of.
- (e) Not to mistake direction (when moving).

**Night Sentinels and Connection.-** A sentinel should be well acquainted with the neighboring posts, as there must be

mutual connection in the line of sentinels. Therefore a sentinel should know the following things with reference to neighboring sentinels:

- (a) The position and number of neighboring posts, both day and night.
- (b) The shortest route to those posts.
- (c) The difference in day and night methods of communication whether by movement or by sight.
- (d) Movements and actions of a post when there is an emergency at a neighboring post.

A clear knowledge of conditions at neighboring posts is essential for the accurate execution of a post's own duties. During the Japanese-Russian War, many sentinels fell into the hands of the enemy while trying to connect with neighboring posts, not knowing that the latter had changed their positions. Again, often the enemy would appear in front of one post and open a violent fire, just as if they were about to attack it; while a hidden detachment attacked a neighboring post and took the sentinels prisoners. The following are the results of our experiences during the late war, concerning the communication of sentinels:

#### 1. Visual signaling; observation.

Flags and other signals.

At night, lanterns. (When behind high ground, simple signals can be sent by disappearing lights).

#### 2. Movements made by a moving sentinel.

- (a) From one point to another.
- (b) Advancing from both sides and meeting at a certain point.
- (c) By a third person (visiting patrols, etc.).

During connection by a moving sentinel, there is a likelihood that the sentinel will be taken prisoner by the secret approach of the enemy, or that he will fall into some danger; therefore, sufficient quiet and caution are necessary. Even though there is danger in always taking the same road, that danger must be disregarded if there is a good road within the line of sentinels. If the sentinel passes by way of the picket, quick communication can be made, but the space intervening cannot be patrolled while connection is being made.

**Night Sentinels and Friendly Patrols.-** When friendly patrols are about to cross the line of sentinels, the latter should be well trained in the proper procedure. The principal points are as follows:

- (a) There must be a spirit of cooperation between patrol and sentinel.
- (b) The sentinel must not be lazy or careless in his duties.

On this point, the following precautions are important:

- (a) The sentinel will inform the patrol concerning what he has seen or heard about the enemy, and all things that the patrol ought to know
- (b) The sentinel must understand the configuration of ground, physical objects, and names of localities in front, so that he can explain them to the patrol.
- (c) It is important that the sentinel know the patrol's duties, its road, objective of reconnaissance, the time and place of return, etc.

When a patrol is about to cross the line of sentinels and advance toward the enemy, the sentinel must not inform the patrol concerning the above mentioned points in a careless or perfunctory manner. The sentinel should regard the patrol as his partner, who is moving out to obtain information, and should do all in his power to assist the patrol in the

proper performance of its duties. On this account, a sentinel, knowing that a patrol is out in front, will be able to judge the importance of rifle shots and other indications that he may hear. When the patrol returns to the line of sentinels, the latter will be informed concerning the following points:

- (a) What the patrol has learned about the enemy.
- (b) Whether or not any unusual signs were observed by the patrol, and, if so, what they were.
- (c) Sentinels will question the patrol regarding designation of terrain, and any other points not clearly understood.

When a patrol leaves the line of sentinels, and advances to the front, neighboring sentinels will be notified by moving sentinels or other means. A patrol is able to carry out its own duty well, by using what it has learned from the sentinel as a basis. That is why it is important that sentinels and patrols should work harmoniously together.

**Night Sentinels and Reliefs.** - Frequently the noise made by the relief, discovers the sentinel's position to the enemy, and this fact will be taken advantage of by a skillful enemy. Again, if the time of relief is known, the sentinel's position will be easily discovered.

Points which will be taught regarding reliefs:

- (a) The amount of noise in transmitting general orders (if the sentinel knows them at the picket, or assembly place in rear, it is not necessary to repeat them every time).
- (b) Cautions at time of transmission-matters relative to watchfulness, etc.
- (c) Movements of new guard to sentinel's post.
- (d) Their posture after arrival.
- (e) Return of old guard and their subsequent movements.

At the time of transmission of orders, as few men as possible will appear at the post. Again, it will be found that some sentinels of the old guard will become inattentive, due to the relaxation of their previous mental strain-such men must be warned. New sentinels, also, on account of the presence of old sentinels at the time of relief, are liable to be neglectful in watching. On this account special care must be exercised, and training is important.

## XXVII.

### TRAINING OF NIGHT SENTINELS.

**Training of Sentinels and Amount of Light.**- The training of sentinels should be carried out at times in which the amount of light varies. That is, on moon light, starry and dark nights, with and without wind, in rainy and snowy weather, etc.

**Training of Sentinels and Terrain.**- It is important that the training of night sentinels should be carried out in all kinds of terrain. In such varying terrain, the power of sight and hearing can be learned, both of which are most important for a sentinel to know.

**Sentinels and Squads.** - Although for the purpose of training, the number of men in a squad should be as few as possible, the time will be wasted if the incompetent Non-commissioned Officers and First Class Privates are placed in charge of the instruction. Trained men who understand thoroughly the ideas of the instructor, should be used for

assistant instructors. Each assistant instructor will be shown the following:

- (a) The squad's sector of ground, direction of operation, and kind of training to be carried out.
- (b) Means and methods of training.
- (c) Time to be employed for this purpose. (d) Position and direction of indicated enemy.
- (e) Signals for assembly, etc.

An Example of Such Training.-First have an old soldier or an assistant instructor execute the movement, while the men under instruction observe it (for this purpose a moonlight night, or just at dusk, is the best time); -next, two or three men will carry out a similar movement, then proceed as follows:

The instructor distributes the sentinels as in the upper sketch, and indicates the sector which they will watch. The remainder of the men are formed in a squad near the instructor and will form reliefs. An assistant instructor will be stationed in the vicinity of each sentinel. The instructor will direct his assistants to oversee the movements of the men while engaged on a certain duty, and to correct their mistakes. The necessary number of men will be sent out to represent the enemy; these men, having been given detailed instructions, will be guided by previously arranged signals (disappearing lights, bull's-eye lanterns, etc.). When all arrangements are completed, the instructor will direct the represented enemy to move, and the sentinels will oppose them. The instructor and his assistants criticize and instruct the men in their duties; or an assistant instructor will form a patrol of two or three men, and, when this patrol has arrived within the vicinity of a sentinel, will instruct the latter how to proceed. When these patrols have already gone out in front of the line of sentinels, they approach the sentinels as an indicated enemy. When the instruction on this point is finished, they change to friendly patrols, and instruct the sentinels upon that point.

**Character of the Training.**- The subjects in which the men will be trained do not differ from those in the daytime, i. e., the principal points are as follows:

- (a) Selection of sentinel's position.
- (b) Sentinel's memory of physical objects.
- (c) Sentinel's method of watching.
- (d) Action with respect to patrols which cross line of sentinels.
- (e) Action to be taken with respect to indications heard.
- (f) Action with respect to the enemy.
- (g) Method of connection.
- (h) Method of reporting.

## XXVIII. NIGHT PATROLS.

**Night Patrols and Methods of Connection.**- Night patrols must be more careful than day patrols in keeping in touch; for in the daytime, even at long distances, connection can be maintained by sight, which, of course, is impossible at night. Special caution is required in the presence of the enemy, as it is then dangerous to use sound for the purpose of connection. Accordingly, the methods which can be used are as follows:

- (a) Diminish distances so that different subdivisions can see each other.
- (b) Use of the whistle.
- (c) Sounds made by striking the butt of the gun, or ammunition pouch.

The limit of communication by such methods is very restricted; therefore, it is often convenient that there be but one group executing a certain movement, but care must be taken that they are not all captured by the enemy at the same time.

**Night Patrols and Methods of Maintaining Direction.** - The difficulty of maintaining direction at night has already been mentioned; the patrol must strive by every means to maintain direction accurately. In order to do this, see those chapters where we have explained how to determine direction, and the chapter treating of the movements of connecting files.

Special cautions in various terrain are as follows:

#### 1. Broad plains.

Movements in such a terrain must be in accordance with the following principles, as great errors in direction arise from small differences in angles:

- (a) Make reliable roads, or a prolonged physical object, the standard.
- (b) Reliance on prominent objects.
- (c) Reliance on the stars.
- (d) Use of the compass.
- (e) Use of maps.
- (f) Reliance on the judgment of a well trained mind.

#### 2. Woods.

It is as easy to mistake directions in woods as in open plains; often it will be so dark that no stars will be visible. The principles laid down under "Broad Plains," are equally applicable to "Woods."

#### 3. Depressions.

After entering a depression, a mistake is often made in direction when going up again on high ground. The following precautions are therefore important.

- (a) Before entering a depression, establish guiding points on high ground both front and rear.
- (b) At the bottom of the depression, especially, make certain of the direction in which you will ascend.
- (c) If necessary, establish other directions, also.

#### 4. Obstacles.

When crossing obstacles, it is very easy to mistake directions even though advancing straight to the front. This is especially true when making a detour; the following cautions will be found important:

- (a) Select guiding points in front and rear before crossing.
- (b) Observe the direction of the obstacle, and calculate its angle with your previous road.
- (c) If necessary, determine the direction anew after passing the obstacle.

## **Night Patrols and Method of Reconnaissance and Passing of Various Terrain and Physical Objects.**

### **1. Woods.**

More minute care must be exercised with respect to woods at night than in day time. The following things, especially, must be borne in mind:

- (a) Don't enter a woods unless unavoidable; on account of its darkness the field of view is restricted, there is sure to be noise, and it is unfavorable for hearing, so pass around the edge if possible.
- (b) When about to enter a woods, first reconnoiter the interior; if possible one man will advance to the edge.
- (c) While in the woods, stop from time to time and listen.
- (d) When the passage is difficult, even though you force your way through, it will usually do more harm than good.
- (e) It is important that one should always expect to run into the enemy.
- (f) The principles already stated in previous articles concerning direction, connection, etc., should be followed.

### **2. Villages.**

Villages are similar to woods, but the following special cautions are important:

- (a) It is a good thing to avoid villages, as a patrol is liable to be molested by dogs, natives, or hidden enemies.
- (b) When about to enter a village, first reconnoiter the interior from the outside; if nothing unusual is seen then it may be entered.
- (c) One man should advance along the edge of the village.
- (d) Seize a native and question him concerning conditions; his attitude should afford some clue to conditions.
- (e) While, at times, it is advantageous to seize hostages, it is disadvantageous to arouse hostility.
- (f) The patrol should pass along the side of the street in shadow.

With respect to the maintenance of direction, connection, etc., see those chapters devoted to those subjects.

### **3. Defiles.**

If a defile is encountered in the neighborhood of the enemy, act in accordance with the following principles:

- (a) As there is usually a hostile sentinel at the mouth of the defile, verify it.
- (b) When about to enter, one man will be placed some distance in rear, and will follow only when the I man preceding him has entered safely. At this time, the patrol leader will be in front, with one man somewhat in his rear, and the third man still further in rear.

### **4. Open country.**

In open country, the following principles are applicable:

- (a) Move with as low a posture as possible.
- (b) Take as much interval as possible; in this case, the patrol leader is in the center, and guides both flanks of the patrol.
- (c) Watch the enemy's direction, and put the ear to the ground and listen for noises.

### **5. Roads.**

In order to avoid being seen by the enemy, march on the side of the road in shadow; if you travel in the center of the road, discovery is easy. The character of the road surface, and its relation to the amount of noise produced, must also be borne in mind. Therefore the patrol, itself, should move quietly, and listen for sounds made by the enemy.

## 6. Gravelly ground.

As much noise is produced while traveling over gravelly ground, special caution is necessary. It will be found disadvantageous for the whole patrol to move at the same time, and halt at the same time; therefore one man will halt, and the other two continue the advance, or they will advance in turn, etc.

## 7. High ground and depression.

High ground is advantageous for vision, but there is danger of being seen by the enemy when descending. When the descending slope is very precipitous, quiet movement becomes difficult; therefore, the patrol should proceed as on gravelly ground. When climbing to high ground, the patrol should halt at the crest line and watch and listen. It is a good thing, too, to stop quietly and listen, before crossing the crest line.

**Night Patrols and Indications.** - When there are suspicious indications, the patrol will lie down at once and listen. Its duty can best be performed if it is always prepared, and discovers the enemy first; accordingly it must avoid moving or firing rashly. As a patrol's movements differ more or less with the nature of their duty, we will discuss each duty separately.

(a) When entrusted with the duty of reconnoitering the enemy's outpost line. When on such duty, if a hostile patrol is discovered, the patrol will lie down at once and allow it to pass. Even though there are opportunities for taking prisoners, the patrol must not allow such side issues to divert it from its true mission. Its action upon discovery of the enemy's sentinels will be discussed in another place.

(b) When reconnoitering the enemy's outpost line, or the position of detachments in rear. The patrol advances as in the preceding case. If a hostile patrol is encountered while on the return journey, or after the weak points of the sentinels have been discovered, it is very important not to make any movement which will discover its presence and thus cause the enemy to change his dispositions.

(c) After the patrol has performed its mission, there are times when it is advantageous to try to capture or kill the enemy. However the patrol's prompt report must not be sacrificed for this purpose, neither must the proper opportunity be mistaken. A plan evolved from the prompting of curiosity or the desire for fame, is not to be commended. No movement should be decided upon without due consideration.

## **A Night Patrol's Reconnaissance of the Enemy's Line of Sentinels.**

### 1. Time for reconnaissance.

The most advantageous times for such reconnaissance are as follows:

- (a) At the time of the sentinel's relief.
- (b) When a visiting patrol passes.
- (c) When a patrol returns
- (d) At the time of the arrival of connecting moving sentinels.

Such times are convenient on account of the noise arising from the movement, and from talking. Therefore, the reconnoitering patrol previous to this time, should have approached the line of sentinels, and have hidden in their vicinity.

## 2. Movements going and returning.

These movements do not differ from those previously made by the patrol against the enemy.

## 3. Methods of reconnaissance.

The patrol being hidden, as we have already described, it should strive to discover the position of one sentinel; this being used as a base will assist in the discovery of the other posts and noncommissioned officer posts. Having reconnoitered the intervening open ground, the enemy's method of security can be verified, and it can be judged whether or not it would be a good thing to enter the line of sentinels. To accomplish this, it is a good thing to follow directly after a passing moving sentinel or a visiting patrol.

**Night Patrols and Quiet.**- Patrols will not fire at night. If they do so, their mission will become difficult of accomplishment, and it will be harmful to succeeding hidden movements as well. Again, patrols will not talk from this comes danger of discovery by the enemy. A patrol's halting, lying down, and hiding, will be without word or sound. There must be no double-timing, or confusion arising from lack of coolness or fear. Only in sudden danger, when there is no other means of escape, or as a substitute for a quick report, may firing be employed.

**Night Patrols and Their Roads.**- Night patrols will vary their roads in coming and going. If this is not done, there is danger of encountering a hidden enemy. If, on account of being on the return road, the service of security be neglected or noise be made, the enemy is liable to take advantage of it. During the late war, a patrol opposite the Shaho river, was in the habit of resting in a certain locality where the men would make a fire. The enemy discovered it, and planted a bomb there. For such reasons, it is especially important to return by a different road.

**Night Patrols and Reconnaissance and Recollection of Terrain.**- As members of patrols will sometimes be used as guides, they will reconnoiter the terrain with that object in view, and their memory must be trained at the same time. While this training is being carried out, the following points will be borne in mind:

- (a) A base for fixing direction.
- (b) The aligning and recollection of places.
- (c) How to pass obstacles, and points to be careful of in so doing.
- (d) The extent of the use of roads and neighboring ground.
- (e) Special marks-such may be made as follows:
  - 1. Scattering white paper.
  - 2. Scattering white powder.
  - 3. Breaking limbs of trees, or trees themselves.
  - 4. Tying on white paper or white rags.
  - 5. Establishing road marks or signs.

The principles governing the recollection of physical objects are similar to those under the section "Duties of Messengers."

## NIGHT HIDDEN PATROLS.

Such patrols hide in important places and discover and report important matters; their movements, of course, depend upon the special purpose for which they are employed. However, under no circumstances, must they make their appearance rashly. The duties of hidden patrols although apparently simple, are not so in reality; success is more and more difficult, according to the importance of the mission. To simply order a patrol to hide at a certain place and only vaguely indicate their other movements, is useless. Whether it is to capture a hostile patrol, or to simply report the approach of the enemy, or to report other conditions (the enemy's movements, etc.), all must be indicated, clearly and accurately. In many instances, hidden patrols will not be called upon to perform duties which other patrols can execute. On the other hand, there will be things difficult for ordinary patrols-such as the recognition of the enemy's night attack, maintenance of close contact, etc.-which must be entrusted to hidden patrols. In such cases, if the patrol tries to capture a hostile patrol, or if they go to the rear to report, their position will be discovered. A hidden patrol, accordingly almost never receives communication or visiting patrols from other bodies.

**Suitable Characteristics for Hidden Patrols.-** A hidden patrol, compared to an ordinary patrol, remains a long time in proximity to the enemy; its members must, therefore, possess the following qualities: Fearlessness, coolness, patience, intelligence and quickness.

Impetuous men quickly become confused and are not suitable for this duty. During the Japanese-Russian War, our hidden patrols on the Shaho river, though they did their work well, were sometimes taken prisoners by the enemy; but they did not capture any of the enemy's patrols.

**Distribution of Hidden Patrols.-** No one should know the position of the hidden patrol but the patrol itself, and the one who posts it. In this connection, the following points will be borne in mind:

- (a) It is disadvantageous for the natives or enemy to know the position.
- (b) Do not loiter about the position unnecessarily before assuming it.
- (c) Remain in another position until dusk, and when it becomes dark enter the true position secretly.
- (d) Other patrols or visiting patrols will not approach or halt at this patrol's position.
- (e) When discovered by the enemy, or by natives, the patrol will quickly withdraw; it will strive to create the impression that it has entirely withdrawn, but later it will assume a new position.

**Position of Hidden Patrols.-** Although the position of a hidden patrol will be in accordance with its objective, the following points will be borne in mind:

- (a) It should be a place from which important things can be discovered. For example, in order to learn of the enemy's advance, it must be in the vicinity of important roads.

- (b) A place convenient for observation, but difficult of detection.
- (c) A place not easy for the enemy to surprise.
- (d) A place where the patrol can send a messenger or signal to its friends without being discovered by the enemy.
- (e) A place not on a road used by the natives.

XXX.

### TRAINING OF NIGHT PATROLS.

**Training and Terrain.-** We have already mentioned the necessity of training patrols on varying terrain. Both sentinels and patrols require such training.

#### **Methods of Training.-**

1. Instruction in the relations between sentinels and patrols.

(a) Preparation.

Having assembled the men to be instructed, the importance of this training will be explained. Distribute instructors and sentinels as in the sketch. The opposing sentinels will be at such a distance that they cannot see each other; in this interval there is space for patrols to move. Time will be wasted, however, if they move too far.

2. Orders for instructors. Each instructor will be informed as to the points in which he will instruct his men. He will be placed in a particular position, and given the approximate time which he can use for one period of instruction. Such training will follow this general method:

- (a) The instructor at B oversees and corrects the patrol's movements against the sentinel, and vice versa.
- (b) The instructor at C acts in a similar manner to d to the one at B.

This distribution having been made, a patrol will be sent out from the squad, first, encountering the sentinel's post A; after this movements has been corrected, the patrol will proceed toward C and B. The officer in charge will send out other patrols at proper intervals, and when the exercise is concluded, will assemble the squad at A; then from the reports of his assistant instructors and his own observations, will comment upon the men's movements.

3. Secretly entering and leaving enemy's line of sentinels.

- (a) Post sentinels as in the sketch; give them simple orders, such as, to keep on the lookout for the enemy, etc.
- (b) Next, send out a patrol to act as a hostile patrol (they should attach a white cloth, or some other distinguishing

mark); this patrol will try to enter the line of sentinels without being discovered.

(c) The instructors oversee the movements of both sentinels and patrol, and judge of the success of the movement.

#### 4. Search for the enemy's line of sentinels.

Having posted the sentinels and attached an assistant instructor to each post, have them carry out the usual duties of sentinels. Their position is unknown to the squad from which the patrols are sent out to search for the enemy's line of sentinels. At this period of instruction, two methods may be employed:

(a) Make an assistant instructor chief of the patrol, the remainder being recruits.

(b) Place an assistant instructor in the vicinity of the sentinels and have them criticize the movement, and furnish material for the officer's criticisms. It is important to limit the patrol's sphere of movement, and thus avoid unprofitable dispersion.

#### 5. Training when meeting hostile patrols.

The instructor, having divided the squad into two parts, attaches an assistant instructor to each squad, and places himself midway between the squads. He carries a disappearing light, with which he signals to both squads concerning the sending out of patrols. The non-commissioned officer in charge of the squads divide them into patrols, and sends out these patrols in the direction of the instructor. Each patrol will be ordered to return to its squad after they have reconnoitered the locality indicated by the assistant instructor. From his position, the instructor watches the movements of both patrols, and corrects them if necessary. When the men have had some training in this movement, one squad operates directly against another.

6. Methods of training in how to pass and reconnoiter terrain and physical objects do not differ in principle from the methods employed in day time, which have already been explained.

## XXXI.

### MOVEMENTS OF A DETACHMENT AT NIGHT.

**Leadership at Night.-** We have examined, roughly, the natural qualities required of the men at nighttime, the next thing is the manner of leadership. The difficulty of such leadership at night, is, beyond description. In turning our attention to this kind of training, one point stands out most prominently-quietness of leadership. At night, as it is important to avoid discovery by the enemy, the men under one's command must be a mass without sound-and this mass must move by silent leadership.

The value of night movements depends upon the amount of skill displayed in silent leadership. Such leadership is attained by the following means:

#### 1. By signals.

These signals will be briefly explained to the men, and may be made by a saber, flag or light; in any case, the following requirements must be fulfilled:

- (a) The signal must be clearly understood by the men.
- (b) It must not be visible to the enemy.

There is no necessity for a great amount of drill in this kind of signaling, because night movements are seldom complicated. Such movements are the causes of failure, and simple movements and consequently simple signals only will be employed. For example:

- (a) Advance-raise the object with which the signal is made, vertically.
- (b) Halt-raise and lower the object, keeping it vertical.
- (c) Lie down-Move the object toward the ground.
- (d) To form parallel columns and advance-a circular motion, or several times to the right and left.
- (e) To form column of companies and advance-A circular movement.

There are several other important signals in which commanding officers will instruct their men in the daytime.

## 2. Method by relays.

The success of this method of silent leadership depends greatly upon the amount of training in peace time. When the voice is used, it is important that it be just loud enough to be heard by the neighboring soldier, and that the rate of speech be as rapid as possible. Although these methods can be accurately executed when the enemy is at some distance, there is always the danger of messengers making mistakes, and delay is directly proportional to the distance from the sender. However, in many cases, the formation at night being the normal formation in column of companies, neither the front or depth will be very great, and, if well trained in this method, success can be expected.

## 3. Method by example.

Soldiers move in accordance with the movements of their leaders; in order that this may be done, the leader must be in such a position that he can be clearly seen by his men. Then when the leader moves, the men move; when he halts, they halt; and when he lies down, they lie down also. Troops can be led comparatively easily by this method; and even though men cannot see the leader directly, they will be able to conform to his movements. The weak point of this method is, that timid soldiers unconsciously affect the movements of others. Therefore in time of peace, the characteristics of each man must be known, and the training must be done with minute care.

**To Accustom Troops to Change of Formation at Night.-** A change of formation at night is attended with various kinds of confusion. Even if this is not the case, it is difficult to carry it out quietly, and slackness is unavoidable. Therefore training in carrying out simple changes of formation quietly and without confusion, is most important. Special training should be given in executing the following movements:

- (a) Column of fours to parallel columns-circular signal.
- (b) Parallel columns to company columns--circular signal.
- (c) Column of fours to company column-circular, right and left signal.
- (d) Column of companies and parallel columns to column of fours-front to rear signal.

In these signals, as a general principle, a circular signal means changing to a broader front; a signal from front to rear means contracting the front and increasing depth of column.

**Individual Cautions in Movement by Squad.-** (See Night Movements of Squad).

- (a) Not to talk.
- (b) Not to hang the head during the march.
- (c) To be careful about connection in the squad; each man will keep his place accurately.
- (d) Each man will see that his clothing and equipments make no noise.

XXXII.  
TRAINING IN SQUAD MOVEMENT AT NIGHT.

**Order.-** First, without arms, proceeding by gradual steps until fully armed and equipped. Very simple movements, as the advance, retreat, etc., will be carried out at first, gradually leading up to complicated ones. The signals should be learned thoroughly in daytime, and, later, executed at night.

**Night Movements and Strictness.-** Night movements, especially, demand the strictest discipline; because, when it is a question of life and death, the influence of darkness brings into being the animal love of life, and there is the fear that supervision may be avoided with consequent loss of power. At nighttime, therefore, slackness must not be permitted. Speed, silence, and strict discipline are essential, and the amount of training will be directly proportional to the degree in which the troops possess those qualities.

XXXIII.  
A SQUAD'S NIGHT FIRING.

**When Carried Out.-**It is a very rare occasion when firing can be executed at night. Conditions must be such that the squad is already quietly halted and have made sufficient preparations, and, while in an aiming position, await the appearance of the enemy. During the Japanese-Russian War, night operations were frequent, but instances when the charge was executed with the bayonet, alone, were few. At the very shortest ranges, a fierce fire was poured in, and then the charge was attempted. However from the standpoint of the offensive, it is a great mistake to prepare for the charge by fire action; as a fundamental principle, the assault of the enemy's position must be made directly by the bayonet. Under really unavoidable circumstances only will an instant's violent fire be executed, and then, under cover of the confusion caused by that fire, dash in with the bayonet. However, if such fire action delays the offensive movement, it will do more harm than good.

From the standpoint of the offensive, however, it is a different matter. Knowing of the enemy's attack, preparations for night firing are completed, a violent fire carried out after the enemy has approached within very short range is most effective; and if this be followed by a counter attack, success often follows. For such reasons training in night firing is very important, especially in the case of small detachments, such as sentinels, non-commissioned officer's posts, etc. When they understand such night firing and make good use of it, they will be able to obtain very good results.

**Important Points in the Preparation for Night Firing.** -In night firing, the men must be prepared in all the following points. The angle and direction of fire should be simple, and the enemy should not be able to avoid it. The methods are

as follows:

- (a) Prepare a rest for the rifle, and in the daytime from this rest, fix exactly the angle of fire, direction, and position of aiming.
- (b) Use horizontal firing.
- (c) Aim by a light from a lantern, bonfire, or other luminous object, or fire by reflected light.
- (d) Fix an aiming object near the muzzle of the gun (auxiliary firing).

**First Method.**-In many cases, prepare a wooden support; that is, in order to preserve the angle of the rifle, fix a fulcrum at front and rear, and from this obtain the angle of fire according to the range. (This is easily fixed by practicing in the daytime.) In short, provide for the two important points-maintenance of direction, and of the angle of fire.

**Second Method.**-This method employs horizontal fire trained individually during peace time. The training will be by squad, and the following cautions are especially necessary:

- (a) Each man to fire exactly to his front.
- (b) Each man's firing to be exact.
- (c) The feet must not be moved unnecessarily.

**Third Method.**--In a small squad, the following expedient may be adopted: Change the day and night positions so that the enemy will appear on the skyline. When the enemy is outlined against the sky, firing can be carried out. However, in large detachments, this method gives the advantage of position to the enemy, which they can utilize to our disadvantage when it becomes light. However, in the case of noncommissioned officer's posts and pickets, good results have been obtained in practice during campaigns.

There are other methods; there is the firing carried out after having caused the enemy to appear in front of a bright light which outlines him clearly. Small bodies can use this method effectively, if they are composed of men who do not fear death. This plan, naturally, requires the fire to be lighted in rear of the enemy, and, of course, great danger cannot be avoided. Flaming shells may be fired, and direct aiming carried out by their light; at short ranges there will be a comparatively large number of hits.

**Fourth Method.**-An auxiliary target is placed in front of the firer at which he aims. Commanding officers must examine the sights strictly in this method.

**Method of Firing.**-Loading the piece after the enemy has approached closely, is the foundation of unsuccessful firing. Therefore officers and men must know the following things:

- (a) To load so as not to be discovered by the enemy.
- (b) Not to forget orders to load, or other orders.
- (c) Not to discover their position to the enemy.

In order to accomplish this, the firer, of course, will load before the enemy's charge. The command for firing will be by signal, or in a low tone of voice. If the enemy hear the command "Aim," they will quickly lie down and thus avoid the flying bullets which come at the next command "Fire." Actual experience in campaign proves this. In small bodies, the following mode of action is advantageous, because I have used it successfully in actual practice:

(a) Have the commands for aiming transmitted from the commander by soldiers nearest him to neighboring soldiers, and so on down the line (in a low tone.)

(b) The commanding officer gives the command for firing according to the size of the detachment and the rapidity of transmission; at this time, those who have not loaded, or those behind time, will not fire.

(c) After firing at the command, the men will load without any special order.  
The above is simply an example, and must not be adhered to, blindly.

**Night Firing, and Collective and Individual Fire.**-- Long continued individual fire is not advisable, for it discloses the position and range to the enemy. In many cases, therefore, it is a good thing to employ collective fire, thereby keeping the men well in hand. Such fire has the advantage of dazzling the enemy's sight by a temporary flash, and then relapsing into darkness, and is thus especially valuable at night. In any case, firing discloses our position more or less to the enemy; therefore, during firing, strict watchfulness is necessary to prevent the enemy from going around our fire and appearing on our flank or rear.

#### XXXIV.

#### METHOD OF TRAINING IN

#### SQUAD FIRING AT NIGHT.

**Order and Methods of Training.**--Train the squad in horizontal firing in daytime; then execute it at night against various kinds of targets. After practice with blank cartridges, train them in battle firing with real ammunition. It is often convenient to carry-out this and other necessary training at the time of entrenching.

#### XXXV.

#### SQUAD NIGHT ENTRENCHMENTS.

**Method of Tracing.**--In tracing entrenchments at night, the following methods may be employed:

(a) Advance as skirmishers, halt, and dig in that position.

(b) Establish soldiers or trees as markers.

(c) Use a tracing line.

(d) Scatter white powder or white paper.

In whatever method that may be adopted, the commanding officer will exercise strict watchfulness, and when he has fixed the position, he will fix the trace according to one of the above plans. It is very important not to mistake the

direction in night tracing, as there are many examples of ridiculous mistakes on the battlefield.

### **Methods Relative to the Line of Trace.--**

- (a) Method in which the ground is occupied in column of fours.
- (b) Method by extension or deployment (in position).
- (c) Method by advancing after deployment.

Although the conditions of the hour will largely govern, on a dark night it is an exact way, to form column of fours to the right or left extending to the markers.

**Night Entrenchments, Cautions for Individual Soldiers and Execution of the Work.**-The above subjects have already been discussed at other places.

**Method of Filling Sandbags, and Entrenchments in which Used.**-In this matter, also, much experience is required. When sandbags are to be used, the following three squads are necessary:

- (a) A squad to fill the bags.
- (b) A squad to transport them.
- (c) A squad to construct the works with them.

Of course it is advantageous to fill the sacks as near as possible to the place where they will be used, but conditions often prevent this. There are various ways of transporting the full sacks. Progress is most rapid when each man works steadily in transporting the sacks from the various places where they are filled, but if the distance be great, an intermediate station must be established, and each man will put down his burden there. Although the method of laying the sandbags will conform to the actual conditions, they will not be laid so as to form pillars, but will be laid generally level like a skirmish trench by gradually progressing construction. In short, in this work, order, connection, quietness and coolness are required, just as in complicated engineering works.

## XXXVI.

### METHOD OF TRAINING

#### IN NIGHT ENTRENCHING.

When the men are well trained in this work, the remainder is a question of leadership of the commanding officer. The order of training is as follows:

- (a) When the enemy is distant, training in the construction is the principal objective.
- (b) Training in the case of the gradual approach of the enemy.
- (c) Training when there is fear of the enemy's attack.

When the above methods of training have been carried out in order, practice will be had in opposing an attack during the construction of the work; or connect this training with some drill in which they will use the works they have just constructed.

## XXXVII.

### TRAINING AND METHOD OF PASSING OBSTACLES AT NIGHT

**Importance of Passing Obstacles by Detachments at Night.**-My experience has been that often small obstacles delay the march at night; and these obstacles are all the more troublesome from the inability to judge their extent, etc., by the eye. On this account, training in crossing obstacles at night is most important.

#### **Cautions for the Commanding Officer with respect to Obstacles.**

- (a) He will inform all men who are to cross of the nature and extent of the obstacle, the preparations to be made, points where lights will be made, guiding marks, etc.
  - (b) Orders concerning method of crossing, formation, rate (pace), distribution, etc.
  - (c) Steps that will be taken to regain the connection that will be lost during the passage of the obstacles.
- The above course of procedure will vary greatly according to the state of the enemy, the weather, and amount of light. Frequently, in crossing obstacles, the column of fours must change to column of files. If great distance is taken, much time will be consumed and connection will be lost.

**Cautions for Soldiers when Crossing Obstacles.** If the men who have already crossed the obstacles try to regain the lost distance by double-timing, they will lose touch with these in rear. Therefore they should be trained in the following points:

- (a) After they have been told what the formation is, they will maintain that formation while crossing the obstacle.
- (b) When obstacles are encountered, if the state of the enemy and other conditions permit, word will be sent back to the rear concerning this obstacle, and a report made of safe crossing.
- (c) The obstacle will be passed without sudden halts or starts.

In the grand maneuvers of 1910, a certain brigade of the Northern Army had to make a night march over entirely unknown country, and the road was only wide enough for a column of twos. On this road was a long bridge-, when the head of the column reached it, they began crossing in single file. The troops in rear did not know the reason of the halt, and, although there were officers at the head of the column, the facts of the case were not learned, and the brigade fruitlessly waited the movements of the head of the column. Now as a matter of fact, the water was very shallow and easy to ford. On account of the darkness, however the men in front did not think of fording. Even though some soldiers who fell in forded it, they did not transmit the news, and conditions remained as dark as before. On this account the march was greatly delayed, and it was after midnight when they arrived at their destination.

## XXXVIII.

### NIGHT MARCHES AND TRAINING.

#### **Occasions When Night Marches are Carried Out.--**

- (a) When executing rapid marches or forced marches.
- (b) When a beaten army is trying to avoid pursuit.
- (c) When attempting to avoid the attack of a superior enemy.
- (d) In order to decrease the effect of the enemy's artillery; to use the darkness of the preceding night to advance to a point convenient for preparing for the attack.
- (e) When about to carry out a sudden attack by taking advantage of the darkness.
- (f) Occasionally used as a substitute for a day march on account of the heat.

#### **Night Marches and Cautions for Staff Officers.--**

##### 1. Consideration as to roads.

- (a) Complete reconnaissance, especially guiding marks, and repairs.
- (b) Determination of methods of passing, going around, and removal of obstacles.
- (c) Steps to be taken to prevent taking wrong roads, etc.

##### 2. Consideration as to troops.

- (a) With reference to connection.
- (b) With reference to the avoidance of sudden halts and starts.
- (c) With reference to the clear designation of detachments.
- (d) With reference to the selection and alteration of formation.

##### 3. Consideration as to security.

- (a) If lights are permitted, the number of electric lights and bull's eye lanterns allowed.
- (b) The manner in which the troops will be led whether by trumpet, command, or signals.
- (c) Whether or not smoking and talking are prohibited.

##### 4. Considerations when halting or resting.

- (a) Too great intervals must not be allowed while resting.
- (b) Troops will not be allowed to choose their own places for rest.
- (c) The men will not throw down their weapons, or other articles which they carry, unnecessarily.
- (d) At the time of moving on, a rigid inspection will be held so that no men or articles will be left behind.
- (e) The time allotted for sleep, no more and no less, will be used for that purpose.

## **Individual Cautions for Soldiers on a Night March.**

### 1. Cautions before starting.

- (a) Clothing and equipments will be properly arranged and adjusted firmly.
- (b) Care will be taken not to make any noise.
- (c) Sleep during the time allotted for that purpose.
- (d) Do not forget or neglect the calls of nature; do not leave anything behind.

### 2. Cautions during the march.

- (a) Be quiet, and do not talk or smoke.
- (b) Remain in the position prescribed.
- (c) Maintain a uniform pace.
- (d) Do not start or stop abruptly.
- (e) Be careful about connection.
- (f) Do not open out in ranks.

### 3. Cautions during a rest.

- (a) Be quiet, and do not talk or smoke.
- (b) Attend to the calls of nature, without fail.
- (c) Readjust equipments and do not leave anything behind.
- (d) Do not rest away from the vicinity of the stacks or the place ordered.
- (e) Keep the haversack near the person.
- (f) Do not sleep except when ordered.
- (g) Do not drink an excessive amount of water.
- (h) Do not enter any house unnecessarily.
- (i) Stay with your comrades and mutually warn each other.

**Night Marches, and Articles Carried by Officers.--** When about to execute a night march, the commanding officer will exercise the greatest care, and will only move after complete preparations have been made. Companies, without fail, will carry the following articles:

- (a) Portable lights (electric lights, or some kind of disappearing light).
- (b) Whistle (officers carry these).
- (c) Compasses (carried by sergeants or attending non-commissioned officer).
- (d) Matches (carried as in (c)).
- (e) In the haversack of each non-commissioned officer, some white paper will be placed, for use in connection duty.
- (f) A small white flag or white cloth (officers carry this).
- (g) Officers will carry, or there will be placed in the sergeants' haversacks, twenty to thirty meters of string.
- (h) In the belt of each soldier, about one meter of string will be tied; it will be convenient in leading them from the rear.
- (i) Usually soldiers will carry a cap cover.
- (j) All watches will be set at time of departure.
- (k) Those who carry a sword will be careful to prevent any noise arising from it.
- (l) In a night march, especially when an encounter with the enemy is anticipated, drum and fife will not be used, and preparations will be made to use the trumpet alone.
- (m) All officers will carry field glasses.

XXXIX.  
NIGHT BATTLES.

**(A) THE OFFENSIVE.**

**The Cause of Success in Night Attacks.--**

- (a) All plans and distributions must be simple, and complete preparations must be made.
- (b) The ground, the state of the enemy, and the weak points of his distributions must be known.
- (c) Our plans and intentions must be concealed.
- (d) Each detachment must be given an independent objective, and absolute uniformity will not be blindly adhered to.
- (e) Our movement must begin near the enemy.
- (f) Make use of the weather, move unexpectedly, take advantage of the enemy's inattention, and utilize any interval he may have left vacant.
- (g) High morale, strict discipline, and excellent training are necessary factors. Also, firm resolution, quietness and coolness.
- (h) The attacker must not allow himself to be hindered by any emergency, or by any action of the natives.

**Causes of Non-success in Night Attacks.--**

- (a) Lack of the different causes stated above.
- (b) When the defender moves on interior lines, and displays skillful leadership.
- (c) When the defender changes his position before the assault.
- (d) The occurrence of unforeseen contingencies.

**Cautions in Night Movements (General Regulations).**

- (a) Things forbidden, and measures adopted for maintaining silence.

Soldiers will not load or fire without orders. Except when necessary, information, messages, speech, all conversation, commands, etc., will not be given in a loud tone of voice. There will be no talking or whispering. Men who have a cough, or who cannot see at night, and horses that neigh, will not be taken along. Take care that no noise arises from ammunition boxes, mess tins, bayonets, artillery wheels, iron chains, etc. Do not take along horses for light baggage. The necessary amount of ammunition will be distributed to individuals.

- (b) Regulations concerning connection.

Attach white cloth or other easily recognizable material to the body or arm. Mutual recognition will be effected by countersign, signals, whistle, etc. There are other methods, such as wearing the overcoat, taking off the blouse, etc.

- (c) Regulations concerning lights.

Be careful of the management of bivouac fires, the prevention of smoking or making lights, and methods of decreasing the reflection from the sword in the moonlight.

- (d) Regulations concerning movements.

Make a clear statement of the objective of the march, the road to be taken, and the method of marching. The method of connection, recognition, the point of arrival, and what to do after arrival there (at such a time, it is difficult for the commanding officer to give commands; if the troops know beforehand what is expected of them, they will strive to do it.)

### **The Commanding Officer and Soldiers in a Night Attack.--**

#### 1. The commanding officer.

In order to be able to make detailed plans, it is important that the commanding officer have a thorough knowledge of the state of the enemy, his dispositions, etc., the terrain, etc. A minute reconnaissance both day and night, must be made over the ground where he expects to move.

The commanding officer must direct the fight, with a determined spirit. His position must be clearly defined, so that information, messages, orders, etc., may be sent and received. Although he must keep his command well in hand, after his policy and plans have been indicated, each detachment must act firmly and independently.

#### 2. Subordinate commanders.

Subordinate commanders will strive with all their might to carry out the task assigned them. They must use their own initiative, in accordance with the plans of the commanding officer. They must understand those plans clearly, and must be diligent in learning everything possible about conditions which will affect their own movements, such as, the condition of the enemy, terrain, etc. They must see that, as far as they are concerned, there is no neglect about keeping plans secret, that regulations are complied with, that the men are kept well in hand, that connection is maintained, and that messages, reports, etc., are properly forwarded, etc.

#### 3. Soldiers.

- (a) They will guard the secrecy of plans.
- (b) They will avoid panic.
- (c) They will comply carefully with orders and regulations.
- (d) They will maintain connection and touch.
- (e) They will not load or fire without special orders.
- (f) Even though fired upon unexpectedly by the enemy, they will not answer the fire, or become confused.
- (g) When the enemy is encountered, they will strive to overthrow him by a fierce hand-to-hand fight.

**Characteristics of Night Attacks.--**A night attack, usually, partakes of the nature of a surprise; accordingly, it is necessary to gain success at one blow, by surprising the enemy. The plans of battle at night, are based on the avoidance of visibility; therefore, the attacker must press the enemy suddenly, and fight a hand-to-hand fight with the bayonet. At such times, a high morale must be united to a firm offensive spirit; because the panic of the defender is much greater at night than in the day time, and the overwhelming menace of the attack will derive a great effect from a sudden appearance.

Such being the characteristics of a night attack, great caution must be exercised to prevent discovery by the enemy, at such a time. When the enemy learns of the proposed attack, and makes his preparations accordingly, the attack will waver and the offensive spirit will become appreciably less. Therefore, noise and lights will be forbidden in night attacks; for noise warns the enemy's ears, and lights warn his eyes. However, sometimes the noise of a night attack is drowned by greater noises, as an artillery and small arms fight in another locality. If the enemy's attention can be

scattered from the front to be attacked by such means, it will have the effect of a diversion; if, on the contrary, it only adds to his watchfulness, it had better be dispensed with.

At night it is easy to deceive the enemy, because of the confusion which arises from the misunderstanding of noises and the lack of vision. Therefore, it is a good thing to carry out a demonstration at the point the enemy expects an attack, and execute the real attack at a point where the enemy does not expect it. The demonstration alone will not deceive the enemy if it is so unskillfully made that the enemy knows that it is a demonstration; it must be executed from the beginning, just like a real attack. However, the false attack not being the main object, it will be modified as much as the necessity for quick reports requires.

**Method of Night Attacks.**--The great disadvantages of night attacks lie in the difficulty of leadership, and the lack of facility in the connection and cooperation of troops. Accordingly, methods of attack which require a complicated disposition, are seldom successful.

Although envelopment, in the daytime, is valuable for both its physical and moral effect, at night, its physical effect is decreased while its moral effect is increased. Of course this movement will be carried out whenever practicable, but its execution will be very difficult. When such a movement is attempted, a combined frontal and flank attack is required; but at night, this movement, also, is most difficult. Things go wrong, and often the movement is not only not successful but our own troops attack each other in the darkness. Therefore, when the configuration of the ground, amount of light, etc., render such a movement at all possible, the greatest amount of care must be taken to see that there is no collision with our own troops. During the envelopment, it will not be necessary for the troops to march a long distance in close formation; it will be sufficient to assume that formation immediately before the charge. In short, the envelopment which is of great value in daytime, is of little value at night. In the majority of cases, the issue will be decided by a frontal charge.

**Night Attack, and Arms of the Service.**--As we have said before, the conditions at nighttime are entirely different from those in the day; so, in regard to the branches of the service, those must be used chiefly which are able to remove the obstacles arising from the darkness. Accordingly it is not wrong to say that night attacks are almost the special duty of infantry.

The cavalry, except when used dismounted as a containing force, will be used only for reconnaissance, security and connection. (There are times, however, when cavalry makes a night attack on the camp of the enemy's cavalry.) In other cases, its function in the night attack is to have all preparations made for quick movement at daylight.

Artillery rarely accompanies the attacking troops. However, there are times when it continues the day firing, or executes the so-called alarm fire by threatening another point; at times, too, artillery firing is carried out in order to deceive the enemy as to our plans. There are occasions too, when the artillery can assist the attack by a violent fire; but, in such cases, the necessary preparations must have been made beforehand in daytime, and the range must be short.

Machine guns are not directly necessary in a night attack, where fire action is not the main reliance for battle. However, when discovered by the enemy, or when fire action is especially necessary, machine guns have an important role. In the battle of Mukden, there was firing on both sides during the night battles, and machine guns, bomb guns, and hand grenades were used. Although, as a general thing, machine guns were used principally in holding occupied points, and for use after daylight, and were taken along for this purpose, they should be held with the reserve until the opportunity for using them arises.

Engineer troops are necessary for breaking up obstacles, opening roads, and for the fortification of positions which have been seized. It is especially important to have such troops during night attacks, as the destruction of obstacles in front of the enemy's position is chiefly entrusted to the engineers.

It is a good thing to have the other branches of the service carry hand grenades, and use them at the instant of the charge.

**The Point of Attack at Night.**--This point is by no means the same as in daytime. In the latter case, the approach is first made under cover, the enemy is then overwhelmed by fire action, and then destroyed with the bayonet. At night, however, the bayonet is employed at once.

As we have stated before, at nighttime, the relations of physical objects differ greatly from the daytime. Therefore the essential elements in the selection of the point of attack naturally differ; the principal points are as follows:

- (a) The ease in which approach can be made.
- (b) The shortness of the distance of the approach.
- (c) The point where the bayonet attack can be delivered unexpectedly.

Not only is it possible to hold the principal point of the position, but a point from which deployment can be made, can be held as well. However, a night attack will not be limited, by any means, to one point. With large bodies, especially, several points of attack must be selected, and independent attacking detachments will be used for each point.

The result of victory or defeat do not extend for long distances as in the daytime; therefore, a victory at one place by no means extends to distant points, and likewise, a defeat has less influence at other points. If these different detachments strive with all their might, independently, they will obtain victory. However, at nighttime, there is so much noise from shouting and rifle shots, that the original objective is liable to be forgotten.

In short, a day attack employs fire action to open the road for the advance; a night attack presses forward under cover of darkness. Therefore, it must be remembered that night movements are easy and secret, and that the cover which is convenient for approach in daytime, must be avoided at night.

**Reconnaissance and Plans.**--The principal factor in successful night attacks is complete reconnaissance. Detailed reconnaissance enables plans to be made properly. Those who plan as well as those who execute, must reconnoiter thoroughly. As far as possible, all officers should be well acquainted with the terrain and physical objects. If the officers who execute the movement are well acquainted with the state of the enemy and the terrain, it will go far in making up for defective plans, and will guarantee success.

Reconnaissance is carried out at night as well as in the day. It is very important to know what degree of relation the terrain and physical objects in daytime bear to those same objects at night. If this point be clear, mistakes and confusion will be avoided at night.

In a night attack, there must be such a self-confidence that success is never doubted. Such self confidence is only obtained through feeling that the plans and execution are the best possible under the circumstances; and that can only be possible when complete reconnaissance has been made. The important cautions with respect to reconnaissance are as follows:

(a) State of the enemy.

His preparations for security, and his distributions. (It is important to know, in detail, the position of the main body, covering position, protective detachments, sentinels' positions, etc.)

The enemy's strength, discipline, customs and peculiarities, also, must be known.

Obstacles and entrenchments. (Detailed reconnaissance as to kind, amount, extent, position, method of destruction of these objects, place, materials, etc.)

(b) Terrain.

Configuration of the ground occupied by the enemy; configuration of ground in front of the enemy's position.

1. The terrain as far as the assembly point and point of deployment; position of such points and roads to the front. The locality in which the advance is to be made, advance formation, method of advance, method of connection and communication, methods of removal of obstacles, etc.

2. Terrain up to the enemy's position. The apportionment of sections for the attack, distribution, methods of removal of obstacles, methods of connection and communication, etc.

3. The influence of weather and the amount of light.

Reconnaissance must be made on dark nights and on -moonlight nights, in clear weather and in stormy weather, in order that the differences in such times may be clearly understood. Too elaborate plans are the foundation of non-success, but it must be remembered that simplicity does not mean just as one pleases. Often carelessness at the time of execution brings discord and confusion.

**The Hour for Night Attacks.**-- The darkness can be utilized until success is attained; after victory, light is essential. This is in order that the fruits of success may be increased through the cooperation of the other branches of the service, the light facilitating the charge and fire action; it is also necessary and convenient for the reconnaissance of the state of the enemy and the terrain.

If it is still dark after the charge, it is most inconvenient for the succeeding movements, and is favorable to the enemy who is well acquainted with the terrain. However the time of execution of a night attack depends upon the objective of the battle, as follows:

(a) The enemy's position have been taken, if it is important to hold it securely, time the charge so as to be able to make dispositions for its defense by daylight.

(b) When it is desired to pursue the enemy after the capture of his position, the movement will be begun so as to be successful at daylight.

(c) When it is desired to attack by cooperation of all arms of the service at daylight, the preparations must be completed by that time.

(d) When it is desired, simply, to throw the enemy into confusion, it should be executed during the night, and the movement must be completed by daylight.

(e) Diversions, threatening movements, etc., will be carried out at necessary times, modified, of course, by the

weather, amount of light, etc. After midnight, the enemy sleeps soundly, and the service of security often slackens. Therefore, under ordinary conditions, begin at midnight and try to finish the movement before daybreak.

**Position when Beginning a Night Attack.**-- (Point of assembly, deployment, etc.) In movements over long distances at night, connection is difficult, and it is easy to mistake directions and fall into confusion. It is therefore important to shorten the distance of such movements. To accomplish this, it is a good thing to advance the point of assembly, and deploy as near as possible to the enemy.

In order to conceal this place of assembly from the enemy and the natives as well, and to stop the movements of the latter, a covering screen against the enemy must be established. This screen must occupy the necessary points before hand, so as not to advance with the main body. If this precaution is not taken, the enemy will learn of the advance of the main body through the movements of the screen.

The point of deployment must be fixed from the conditions of the hour. The following points govern the selection:

- (a) Amount of the enemy's service of security.
- (b) Terrain.
- (c) Size of our army.
- (d) Degree of darkness.
- (e) Weather.

In short, it is advantageous to have it near the enemy, just so that it will not be discovered, and in a place convenient for movement.

The British Field Service Regulations fix this distance at not nearer than 900 meters. If the ground is level and open, the assembly will be made in a deployed line at once, as a substitute for the assembly in column of march. Even when this is done, the zone of movement will be divided, and all detachments will advance in parallel formation. This is especially true when the movement for attack must be carried out from a long distance. When already near the enemy's line in daytime, or when already deployed near the enemy, the night attack can be begun from this line. The main thing is to make the advance easy by deploying as near as possible to the enemy without being discovered. The points of assembly and deployment, roads to the front, etc., will be marked as far as possible, by paper, rags, broken limbs of trees, or soldiers as markers. It is a good thing to block up the wrong roads, branch roads and unimportant roads.

**Night Orders or Instructions.** -- Orders for a night attack will be based on the usual orders for a day attack. However circumstances may arise at night which make it necessary to violate regulations. The Infantry Drill Regulations say, "In the order for a night attack, there will be indicated the object of the -march of each detachment, the road, together with the method of mutual communication, the method of recognition, and, if necessary, the point of arrival. Again, it is advantageous to indicate, beforehand, the first step after this movement. "

If the order be made simple, it is especially necessary to supplement it by instructions. There are two kinds of orders necessary, depending on the distance to be traversed for the attack, viz.-the orders for the march to the assembly point, and the orders for attack. If necessary, both matters will be included in one order, or the order will be made as conditions develop. Orders from superior headquarters usually include both points in one order; the officer who is to execute the order, will divide it into two parts, and give the necessary orders. In the night attack against Kyucho during the late war, the men were told the general tenor of Major General Okazaki's orders; these orders did not differ greatly from the usual day order, but the principal things desired were explained by instructions.

**Distribution and Formation for Night Attacks.**-- The formation for the night attack must be simple. According to our regulations, company columns in parallel lines are used (line of company columns); or detachments covering from front to rear (for example, battalion column, or double column of companies). Sometimes a few skirmishers are sent in front, and sometimes, not.

Although the line of columns is very advantageous as the greatest number of bayonets can be employed at the time of the charge, the movement is very difficult when the distance to be marched in battle formation is very great, or if the terrain is not very favorable, or if the night is very dark. The advantages and disadvantages of the battalion in column, are directly opposite to the above. The double column of companies is midway between the two above formations, with corresponding advantages and disadvantages; this formation is therefore most often used in night attacks.

However, the selection of the formation is largely governed by circumstances; each company must conform to the conditions of the hour in adopting the company column (column of platoons), or the parallel columns. While the latter has less masses strength than the former, the march is comparatively easy. Therefore, it is a good thing to use that formation while marching, and change to the other when conditions require it.

According to the state of the enemy and the terrain, the attacking troops, in depth of column, are divided into two or three echelons. Even when there is fear of a counter-attack from the flank, the division into three echelons will be made, the second echelon being placed in rear of the dangerous flank of the first; the third will be placed directly in rear of the first so as to make certain the success of the first line. It is important that the distance between echelons should be short. If it is believed that there will not be strong resistance at the point of entry, but that it is probable there will be a strong counter-attack after entry, it is important to make the rear detachments very strong. On the contrary, if it is believed that the enemy can be beaten at the first entry, the first echelon will be greatly strengthened.

Even in a night attack, a reserve cannot be dispensed with. If it is anticipated that the fight will continue until daybreak, an especially strong reserve is important until in many cases it must be placed very near the first echelon. Usually, when the attacker's first line charges the enemy, its formation is broken up; this is true irrespective of the strength of the enemy. The ranks must be reformed at once, and it is the duty of the reserve to cover this movement and repulse the enemy's second line. The reserve, often, by an unexpected attack, can cover the retreat of the first line.

**The Advance to the Attack.**--When this advance begins, the troops must resolve most firmly, to be silent and quiet. If the troops can be led by signals and without the use of the voice, it is most advantageous. Each detachment must maintain the direction of the march accurately; to do this, the following principles must be observed:

- (a) Select well defined marks, fix intervening marks, and follow them.
- (b) Follow along roads, railroads, ravines, or edges of rivers, which prolonged, reach to the selected marks.
- (c) Send out scouts; establish soldiers as markers, sign-posts, etc.
- (d) Use military or civilian guides who are familiar with the route to be traversed.
- (e) Fix the direction by compass, stars, portable electric lights, etc.
- (f) Maintenance of connection.

Each detachment will preserve connection and cohesion; unexpected incidents must be treated coolly; if the enemy's sentinels are encountered, capture them (without firing) or kill them with the bayonet, but it must be done without noise. In order to recover connection and order, halt from time to time. When each detachment has arrived at the attacking point, it will maintain order and quiet all the more, and will advance most carefully.

When the enemy's effective fire is encountered during the march, or when discovered by his searchlights, it is a good thing to halt temporarily, in order to decrease the effectiveness of the fire, or escape the enemy's vigilance. Care will be taken, however, not to retard the forward movement.

**Night Attacks and Firing.**-- A night attack should be a surprise. However, even though the attack may be successful, it must be remembered that the enemy, when he fears a night attack, will take sufficient precautions and make preparations for fire action; therefore, never think that you will always be able to enter his position undiscovered. On the contrary, rather expect to be discovered; and the chief thought in your mind should be the necessity of a desperate effort in order to carry out your mission. The attacker must, therefore, be prepared to receive the enemy's fire; that is, he must be firm under that fire, and come to close quarters with the bayonet.

Night firing will not have a great effect if the attacker's movement is carried out properly; therefore, even though the enemy may open fire, it does not mean that the attack is a failure at once. On the contrary, success or non-success, depends upon the attacker's succeeding movements. For this reason the troops must not be thrown into confusion by this fire, but must quietly continue their movement. Silent intimidation will make the enemy believe that there is not a single echo to their fire in the darkness. It is of special importance in night attacks to increase the enemy's doubts and fears. If their fire is returned, the following disadvantages result:

- (a) It discovers the attacker's strength to the enemy.
- (b) It discovers their position as well.
- (c) The enemy will discover the real front of attack, and will be able to make his dispositions accordingly.
- (d) Silent intimidation loses its effect.
- (e) It decreases more and more, the charging strength.

Therefore, by firing, the attacker destroys himself, does not injure the enemy, and the man who believes he injures the enemy by such means, is destined to failure. While in daytime it is necessary to open up a road by such means, when it is remembered that this is unnecessary at night, night firing will become meaningless. How much more true is this when the fire is due to the enticement of the enemy and is defensive in nature. One can say with truth, that night firing on the part of the offensive means failure.

Night firing by one detachment encourages meaningless fire at other places, and such things denote clearly the inferiority of an army. Therefore, the highest officer down to the private soldier must brave the enemy's bullets and long for the charge.

However, at times, firing is used to cast down the enemy's morale; this is only done when an entry into their works is certain, and is never done to provide an opportunity for entry or to open the way of the advance. Its function is to increase the success of the charge and to dazzle the enemy, this purpose being best effected by the use of hand grenades. This is but the matter of an instant, and the attacker must already be in the position when the grenades are used; they will then rush forward shouting the battle-cry, and success is certain. Sometimes, firing may be used as a substitute for hand grenades.

**Preparations Against the Defenders' Changes of Disposition.**-- The defender, in considering a night attack, takes the following steps:

- (a) Complete preparations for night firing.
- (b) Illumination.
- (c) Change of position.
- (d) Counter-attack.

Therefore, it is important that the attacker be prepared to take proper steps to meet such actions. Against fire action, as we have already stated, lie down temporarily, or avoid the direction of the line of fire. (The enemy's firing line at night,

on account of the necessary preparations, is often fixed). If illuminated by lights, lie down and keep still, in order not to make a shadow and to make the target as small as possible. It is important to avoid gazing at this light, for, if this is done, it will dazzle the eyes.

The defender, at times, will leave a weak detachment in the day position, and occupy a night position with his main force, and often this old position is attacked at night. When the attacker discovers this, he should make his plans beforehand, and not fall into the enemy's snare. The attacker should not take it for granted that the defender always occupies his day position at night.

When it is discovered that the defender is not in his day position, occupy that position with service of security troops, reform the ranks and scout to the front and flanks. Rear detachments should be called up, and emergencies provided against.

Sometimes when the enemy knows of our advance, he will make a counter-attack from a flank. Therefore, do not stop at simply providing for the service of security on the flank; make such a distribution that you will be able to oppose any emergency that may arise.

With reference to the destruction of obstacles, see the section on the attack on strong positions.

**The Night Charge.**-- A charge at night is the penetration of the enemy by the power of combined wills and a high morale. This charge must come unexpectedly, and with an overwhelming impulse. The enemy must not be allowed to await our coming with rifle in hand; we must seize the position in an instant, and must have a collected detachment to hold the position when the enemy, awakening, strives to resist. If the enemy open a violent fire and we stop to answer it, our movement will end in failure, and the movements of other detachments will be checked by the fire of one detachment. Therefore, no attention should be paid to the enemy's fire, but the charge must be continued without hesitation. To accomplish this there must be a self-confidence on the part of the commanding officer which expects success, and the subordinates must have confidence in their commander.

**Movements after a successful Charge.**-- When the charge is successful, each detachment quickly reforms, takes strict precautions for security, provides against the enemy's resumption of the offensive, and pursues as quickly as possible.

When a position is once taken, it is necessary to make preparations against receiving the enemy's violent fire from every side as soon as it becomes light. Again, preparations for defense must be made very quietly. This makes it difficult for the enemy to plan the resumption of the offensive, and will make it difficult for other detachments to judge how to change their dispositions according to the existing state of affairs. Therefore, after a successful night attack, shouts of victory and noisy confusion, will disclose our position to other detachments of the enemy, and will be the cause of our being fired upon and reattacked.

**Pursuit After Night Attack.**-- Even though the night attack be successful, it is not good policy to leave the position suddenly and pursue the enemy, because of the many disadvantages resulting from the fact that pursuing fire cannot be carried out, the great amount of confusion, and the fear of receiving the enemy's counter-attack. It will be found difficult enough to hold the position, even. This is especially true when the position captured is only one section of the enemy's line, his other detachments holding their previous positions. In such cases, it is usual to make preparations for taking up the pursuit, and await daylight. When the pursuit can be taken up without fear of the above mentioned disadvantages, the success will be correspondingly great.

## (B) THE DEFENSE.

**Psychological Disadvantages.**-- At night, the defender has a feeling of anxiety, because the surrounding obscurity prevents the vision, which is so necessary to him. His principal mode of defense is fire action; and while that is very dangerous to the offense in daytime, it cannot stop the charge at night. Therefore, it is the duty of the offense to increase the defender's doubts, fears, suppositions, etc., and make a demoralized army more so.

For such reasons, the commanding officer of the defense must always strive to maintain good morale, quietness and coolness. How much more must he strive at night to force back the individual weaknesses of the individual, which arise on account of the difficulty of supervision. To do this, he must maintain a close formation which is convenient for leadership and which enables him to use the psychology of the mass.

The reasons for the difficulties of the defense are as follows:

- (a) The difficulty of preventing the approach of the enemy by fire action.
- (b) The difficulty of knowing quickly of the approach of the enemy and, consequently, taking proper measures against him.
- (c) The difficulty of mutual assistance, on account of each detachment being bound down to its place.
- (d) The fight is one of localities; other troops waste time (difficulties of leadership, cooperation, movement).
- (e) The ease in which a defender falls into a feeling of being at a disadvantage.

**Action of the Defense at Night.**-- On account of the above mentioned disadvantages, the defender must adopt measures to offset them. He must, therefore, take the following steps:

- (a) Guard against the approach of the enemy by sending out detachments in front of the defensive line, by distribution of hidden patrols, by establishing electric bells, alarms, etc.
- (b) Light up the ground in front, discover the enemy's approach at a suitable time, and make such approach difficult.
- (c) Fix obstacles at important points in front of the position, and prevent the enemy from destroying them.
- (d) Make preparations beforehand for night firing in the direction of the enemy's attack. Especially, provide machine guns at points where it is possible to enfilade the roads by which the enemy will advance, and make complete preparations for firing.
- (e) Obstruct, by offensive movements, the approach of the enemy, and his engineering works.

When it is discovered that the enemy has approached closely and has constructed works, obstruct him by the attack of small detachments. The objective of such a sortie, of course, is not the same as that of the main battle which drives off the attack. It is therefore, not only not necessary to use large detachments, but when such are employed it is liable to give rise to a battle not planned for. As for the reasons for not always carrying out a sortie, all depends upon conditions as the time.

**Steps when Anticipating the Enemy's Night Attack.**-- When the enemy's night attack is anticipated, have a formation ready to oppose him. Whenever the dispositions have to be changed at the time of the attack, leadership and movement are difficult on account of the darkness, and mistakes and confusion will arise. Accordingly, when expecting the enemy's attack, the following steps will be taken beforehand:

- (a) Strict service of security.
- (b) Place the necessary number of men in the firing line.
- (c) Troops in rear should be called up near the firing line.
- (d) Take necessary measures for connection and communication. (Distribution of lights, markers, etc.)

**The Defender's Night Battle.--** The defender, at night, will not permit a single soldier to leave his position. Each detachment will guard its assigned position, independently. Even though one section may be taken, no time will be wasted in reattacking it by rear detachments. Detachments in the first line must remember that it is generally impossible to count on assistance from neighboring troops or troops in rear. The defense will strive to destroy the enemy by sudden violent fire from the shortest ranges. To do this, after preparations have been concluded, await the approach of the enemy; when he is very close, open up a violent fire, and throw hand grenades. At this instant, use the bayonet in a determined counter-attack. The enemy's random and searching fire at long ranges must not be answered. Premature fire action causes useless firing to start along the whole line; it is not only noisy and useless, but it discloses our position to the enemy, as well.

At night, except for the protection of a locality, a delaying action will hardly be carried out. In this case, also, as large a reserve as possible must be kept in hand especially when there is the fear that the engagement may last until daylight; if there is no reserve then, the day battle cannot be continued.

**Steps When the Defender Drives Off the Enemy.--** When the enemy is repulsed, the defender reforms his ranks, but very rarely pursues with his whole force, as in daytime. Usually a small detachment from the reserve, or, at times, simply patrols are sent out (according to the French regulations, only pursuing patrols) who follow the enemy only. The remainder must guard the position firmly, as before.

Even though the defender is certain that the enemy's charge will be successful, he will not heedlessly withdraw from his position. This is because a night retreat gives rise to extraordinary confusion. A detachment which is pursued by the enemy, will again occupy a position in rear, and detachments not yet defeated, will remain in their former positions. Taking advantage of the latter's success, the defeated detachment will await an opportunity for a counter-attack on the flank or rear of the enemy who has penetrated into our lines. A general retreat, or a general reattack, however, had better be done in daylight

Thank you for reading our special military manual reprint  
Visit [Resist.com](http://Resist.com) to buy future and archived editions.

**Sure you can trust the government, just ask an Indian!**

We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to [TM\\_Metzger@yahoo.com](mailto:TM_Metzger@yahoo.com) (Note the “\_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

**Tom Metzger  
P.O. Box 401  
Warsaw, In 46581**

**24 HOUR ARYAN  
HOTLINE  
(574) 267-5036**