THE FUNDAMENTALS OF COUNTER-SURVEILLANCE
By: Moddy
Ver. 1.0

Author's note:
This wasnt intended to be quite as paranoid as it turned out to be, I'm not 100% sure on it really. It was something I was interested in and I couldn't find any documents whatsoever on it - so I thought I'd put what I know down on paper!

Compiler's note:
This document was originally posted on night-ops.net. The PDF version of this document was compiled and formatted by Secant. No content was added, removed, or modified.

Introduction

Lets clear a few things up - By no means am I an expert on this, on all accounts - everything I know has either been improvised when required, read from books on the Security Service(s) or adapted from the media. I have never read any specific counter-surveillance manuals or documents, and I am only writing this due to the sheer void of such material.

I came to research CS due to situations I found myself in where I was being pursued by people who were after me due to, largely, situations I made myself. These ranged from pissed off people that weren't happy about decisions I made, a drug dealer who didn't like me making a stand about the mental health of my ex-girlfriend and my own paranoia when I was researching Pyrotechnics and HE, and later researching certain aspects of the internet/anonymity networks.

When I was trying to gather this information I found it incredibly hard to gather, so I decided to compile anything I could think of - or anything which I have done. This may not be of much use for this community as a whole, but I figure you may have your own words of advice or techniques you wish to add - and some of you may have situations to apply it too.

First of all, we'll start with what CS is. In simple terms, its the avoidance of surveillance and the methods of which one may take to minimise the risk of surveillance. Its uses can range from (as in my case) "covering yourself" from people who may wish to take negative actions against you, to activists or political advocates who may also have wronged people. It also applies to those who feel they may be under surveillance by official means - i.e Law Enforcement.

Before we delve into CS; it may be worth taking the following into account:

* Your security is only as strong as your weakest point - there is no point investing time and effort into securing yourself from surveillance if you're broadcasting your activities and movements via insecure electronic means. (Plaintext websites, Email, Phone, SMS)
* Having compromising items on you can ruin even the best of silences. (Unencrypted USB disks, notes, documents..)
* A comprehensive security plan is not going to be an easy thing to accomplish, and can take weeks to implement depending on your past

Introduction to Personal Security
Whole books could be wrote on Personal Security (PERSEC), however - I aim to give you the bare minimals to take care of yourself from here on. I am a hypocrite, and need to follow my own advice. Once again, this document was mainly to serve my own purpose of allowing me to get my own plans into focus, and to approach my own situation from the perspective of a third person - so I can fully understand any concerns you may have at this point.

First of all, we need to approach this as if our life is a room. In this room we have many items which we don't want to fall out into the hands of those who we don't trust or know. The first thing we need to do then is clear out the room - have a massive tidy up. So we need too first correct our ITSEC (Information Technology Security) -

1. Set up multiple email addresses.
- Real name for social networking, banking, family and friends..
* Secure password
- "Handle" for internet activities marked "A". "A" is completely safe.
* Secure password
- "Handle 2" for internet activities marked "B". "B" is anonymous.
* Alphanumeric password; 9+ characters
* PGP Encryption

- Also, Set up multiple ICQ or MSN accounts.
* ICQ can be better due to the fact the username is a random string of numbers.

2. Correct our security settings
- Install add-ons for your browser - NoScript etc - before correcting your browser settings (Use Incognito mode, have firefox prompt to delete all data after every use.. etc)
- Ensure your Operating System is up to date, firewall software is correctly set-up and have malware protection
- Un-install any unrequired applications
- Perform full system scans for any nasties

3. Build upon the foundations of our security
- Install TrueCrypt - Available for Mac OS X, Windows and *nix
- Get a disposable USB pen drive and use as a TrueCrypt partition

- Install TOR and Privoxy - Privoxy has some nice features even when not in use with TOR (Check your TOR set up is working correctly, with anyone of the numerous online checkers)
- Grab some encryption plugins for your favourite Instant Messenger
- Perhaps begin to look at VPN (Virtual Private Network) solutions

4. Begin sorting through your data
- Move ALL sensitive data to your TrueCrypt disk, ensure you have a secure passkey THAT YOU CAN REMEMBER
- Delete all data you don't need. You know that folder you haven't looked at in a year? You have lasted a year without it - you don't need it now. DELETE.
- Think about using an app like CCleaner to clear your system of all temp files, clean the registry..

5. Utilising your new email addresses
- You know all those forums you frequent? They all let you change your email address, and if they don't - you don't really need them anyway, do you? Now sticking to the "A" and "B" classification - set them to the correct email addresses.
- Those Social Networking sites - those need to be classified too. Classification "A" can probably be roughly linked to your real ID if you feel the strange urge to have people from forums on your facebook - but doing this is a slippery slope. (Trust me. I'm there right now..)
- The old email addresses may be worth checking for another week, and maybe going through your contacts selecting those who *really* need to know your new email address (Whichever you choose to supply).

6. Going through the long process of cleaning up your past
- Do you know EVERYONE on your facebook? No? Well, enjoy going through all 200+ of your friends and deleting every person you don't know, or don't trust. Oh, I hear you say you don't enjoy only having 16 friends.. Tough.
- Look at your photobucket, myspace, facebook, twitter, youtube, livejournal.. anywhere you upload pictures or text. How much of that is actually a good idea to be giving away? Time to start mass-deleting! (Lovely living in this day and age of vast social networks and web2 websites isnt it?!)
- Google your name. Google your handle. Don't like what you see. Try and change it. Good luck though..
- Check out Google Dashboard; it has search histories and everything for you. Clear it. Now. Go.

7. Estabilish a security routine - and stick to it
- Before we start out security routine, we need to wipe all the free space of our hard drive, preferably multiple times to just try and make any data recovery that bit harder.. There are many tools out there to do this, you if you're on *nix you can always dump the contents of /dev/random into a file.. until the file get too big and errors out.
- To ensure we stick to this routine we can't set stupid targets like doing a full system clean every evening; once a week is a good amount of time; and complimented with common sense you should be fine! This weekly clean should involve:
* Full malware scans
* Cleaning of ALL free space on the system

Note, you may want to install truecrypt - copy all your data over to a USB disk encrypted with truecrypt before erasing (secure deletion) your whole hard drive and re-installing the OS and starting a fresh. Your truecrypt partition will be able to be read by any truecrypt installation - so this will work!

Also, I've worked as a Hardware Technician - LEARN TO FIX YOUR OWN COMPUTER. Don't trust ANYONE going near it to try and fix it, or repair it in anyway. Fixing computers is easy anyway, even if it means buying a simple book on the subject - just learn to become utterly self-reliant with things like this. The same goes for mobile phones.

Additionally, you may wish to ensure you have a decent BIOS password set-up to stop anyone from booting up your system from a live distribution and copying data over. This means you need to ensure your hard disk is #1 in the boot priority. They could, just remove your hard disk then - so you may want to get a computer case that allows you to use a lock.

Another way of protecting your data is to use the "FDE" (Full Disk Encryption) feature of Truecrypt which encrypts the entire hard drive. Windows 7 wont work with this, UNLESS you do some magic to the partition table prior to installation. (Google for instructions. Basically windows 7 creates an emergency partition which stops truecrypt from working - but Windows 7 wont do this if theres already a partition table; so you create 2 partitions yourself, install windows 7, delete the spare one, and make the windows 7 one bigger..)

Now please note, that is far from a fully comprehensive plan for your ITSEC, but it should have given you more than enough food for thought to get into a secure routine and to clean your system. Now we have a secure system we need to consider the fact its going to be communicating with systems on a insecure and vulnerable network - let me introduce you to our new best friend; COMSEC, or Communications Security.

We have to remember our system is meerly a peer within millions of, often insecure, peers. With this in mind we need to do everything to ensure that those which we communicate with are adhering to similar guidelines; and if not - we're only communicating with some ability of anonymity. To do this we may need to think about..

- Virtual Private Networks; Do we require a secure gateway where even our ISP can't see what we're doing? If so, do we also need to keep speed up to an acceptable level? If so; a VPN maybe for us. All traffic can be routed via a VPN which is also nice when considering things like file sharing and email.
- Install Messaging Encryption; There are many encryption applications out there for IM. One of these is OTR, OTR provide support for several popular clients. Please note; OTR is closed source and I cannot confirm the security afforded by this! (Aim for open source solutions if possible)
- Email Encryption; Ensure anything of secrecy is sent between encrypted peers using PGP Encryption. GNUPGP is available for free, and there are many resources available on the internet regarding the setting up procedure. There are also firefox add-ons available to interface GNUPGP with Gmail in Firefox.
- Email and IM Anonymity; should you choose to run a VPN then this will be fine - as all your IM and Email traffic will be routed via that. However, if you don't then you may wish to route your IM applications via TOR - although TOR is not secure, it is anonymous - and security should be covered with your encryption!

Now thats the obvious methods of communication covered. Lets cover the traditional types;

- Mail. Do you even use this anymore? As far as COMSEC goes you may want to be careful about handwritting, but similarly you may want to be careful of printer signatures.
- Telephones. Get a Pay as you go SIM card, a disposable phone and use that. Gaurd this number with your life and keep it seperate from your personal phone/number. If you use a smartphone, limit the amount of apps you install and make sure things like the Google tracking service are OFF. Bluetooth? Off. Be prepard to dispose of this number at any time, if you can afford, get a new SIM card every 2 weeks or so - 99p stores have a variety of SIM cards in the UK. Ensure you have a PIN code, contacts are named discreetly, and the phone requires the PIN code to unlock.

Now we have the basis of PERSEC (ITSEC + COMSEC inc.) covered - its time to meet our good friend Operational Security (OPSEC). This is all very specific to what you are doing -

however the objective of operational security is to ensure that your operation isnt compromised by any information leaks, and that only trusted people have trustable amounts of information.

The most obvious approach to this is to not tell anyone about what you're upto, keep notes on your USB encrypted pen drive and keep your wits about you. Generally, PERSEC and OPSEC overlap quite a bit, as do most of these security disciplines.

Before we get on to the Counter-Surveillance it may be a good time to look at your own Physical Security. Most of us on this forum know quite a bit on Physical Security so I wont waste my time going on about locks, deadbolts, chains, window locks, ensuring you can't card your way in...

However, some of us may wish to consider leaving traps around should anyone get in. Even simple things like leaving items in specific spots, taking photos and comparing them. Or sellotaping a peice of thread to the back of a drawer, to the back of the chest of draws - meaning if anyone opens the draw then the thread will be ripped off.. You can use your imagination and go wild with these ideas; but they may just help you find out if someones been having a nosey around your stuff!

Part 1. Identifying the threats

What threats does Surveillance pose to you? Or more specifically - WHO pose these threats? For many of us it may be Private Investigaters hired by people who may be pursuing civil cases against us - maybe Trespass. Or you may be linked to someone in a complex divorce case. Or maybe something a little more dark? Police and other Security Services? Perhaps you fear you're being watched by a stalker.. the possibilities are endless, and the reasoning can often be sinister.

Once we have identified the threat, and the opponent who poses this threat we need to ask;
- What would be the most damaging they could find?
* Perhaps meeting with a specific person?
* Maybe seeing you within a specific location?

- What avenues can they persue me through?
* Electronic - Social Networking websites, Forums, Email addresses, Gumtree/Craigslist postings
* Physical - Surveillance of your person, address and assets.
* Communications Intercepts - Landline interception (a la beige box), Mail intercepts, Network traffic sniffing

- What are they trying to find?
* A relationship
* Evidence of activities
* A personal profile

- What will they try and go for next?
* Observation of friends and known associates
* Tampering with your property
* A physical attack

Once you can identify just who you're trying to protect yourself from, you can begin to view yourself with their own eyes.

Part 2. Identifying patterns of behaviour

You go to work everyday - wake up at 6am, leave the house at 7am, catch the 0718 train... Most of us live surprisingly uneventful lives between Monday and Friday. This makes the job of surveillance a lot easier, by identifying patterns in your everyday life it becomes easier for an observer to identify changes in your activity, identify your mood or feelings and ultimately, it allows them to second guess your every move and determine where you are at a given time.

- Try and take different routes to get to the most mundane of places. Try and get in the mindset of "exploring" your surroundings and finding new ways to get to B from A, even if it means going through C.
- Identify your usual schedule and work out how you could mix it up - preferably try and work in some busy places. Shopping malls, markets, pubs, buses..

Think about places you often go in your spare time - friends houses, bars and clubs.. How do you get there? The same route everytime. There is likely to be a point of the journey where an observer could determine were you are going to go. Although even if you spice your journey up - a good surveillance operative will be able to still see you get to the destination; the whole point is to inconveniance them and make their lives that little bit harder. (Unless you wish to present an easy target who is oblivious to any surveillance)

- Try getting off buses at different stops and walking for 15 minutes or so, spicing routes up and wasting time.
- Determine when to travel based on how busy it will be. Ever played "Where's Wally?", it's quite difficult at times isn't it? Use this when planning meetings; its easy to get lost in a crowded place - and much harder to eavesdrop. (Although you never know who you're barging past..)

Look at the way you dress, the things you buy.. How many times have you got on a train or a bus and seen someone dressed in a suit, clutching a specific paper and thought "Another city worker..". Its a stereotype, but its also very valid. This also applies to YOU. Do you favour certain items of clothing for certain events? I personally favour a specific pair of shoes if I'm going to a social event, a pair of canvas ones if it's just meeting a friend, trainers if I'm doing something.. erm.. risky. Now that fact alone gives anyone reading this enough to determine what I'm up to based purely on one item of clothing. Bear this in mind!

- This one can be quite a hard habit to break, but its a valid observation - people WILL pay attention to how you look.

Part 3. Profiling your associates, their trust worthiness and creating your own profile
This is one of the harder things to do - it often means making harsh judgements on those you feel the strongest about. However, following on from PERSEC - you need to determine who knows what about you, and how trust worthy they are. Now this goes beyond the usual "friends trust" that you are familiar with..

- Would this person be able to handle themselves should something I say to them get them in trouble?
- How much do they know of me already, would they expect it?
- How likely are they to tell anyone? When drunk? To impress a girl?

Often, its best just to tell people what they specifically need to know - if anything.

- "I'm gonna be going out tonight at about 10 mate, you couldn't give me a ring when I get back at 3 could you? If I don't answer then could you..." - AKA "I'm doing something a little risky, if I dont answer I could be in trouble."
- "I'm meeting up with another mate, you wont know em" - AKA "I'm meeting someone that I don't really wanna talk about"
- "*silence*" - AKA *anything you're not sure about*

Even friends who have the best intentions can pose problems if they get in out of their depth, and often its just a whole lot easier to tell a few white lies and keep things simple. In some ways - you owe it to THEM not to drag them into this.

This changes however if you think the surveillance is very real, and they may try approaching friends next.

You should also think of profiling any friends prior to informing them of anything secretive.
- How do they come across?
* Straight A Geek or Street smart crook? Sometimes the geek is better..
- What do they enjoy?
* Think of their interests
* What do they read? Talk about?
* What do you usually see them doing?
- Who do they associate with?
* What type of people?
* What type of places?
* Any threats or trouble?
- Where are they usually found?
* Workplace?
* Pubs/clubs?
* Friends?
* Girlfriend?
- Disadvantages
* Confidence?
* Lies?
* Nerves?

By profiling them you can make sure you are doing the right decision by informing them, and you can also look at their own weaknesses and ensure that you can pre-empt any next move.

Now you have profiled some of your friends, we need to profile you! Think about those above questions and answer them, then determine what bits can be "public" and which bits are certainly "private". Make sure you drill this profile into you, it needs to be second nature. You can't risk answering questions with different answers at social occasions, nor can you risk different people knowing different things. As far as everyone needs to be concerned - you're a bog standard normal guy with a boring normal life. End Of. All you need to do is work out the specifics of this cover.

Part 4. Avoiding Surveillance

Heres comes the fun, hands-on, ducking'n'diving stuff! Let me re-affirm the fact that this isn't a speciality of mine, but merely a topic I feel we're woefully lacking information on! With that said; lets get on with it.

- Always use different routes from A->B.

This has already been covered above, but I can't explain just how useful this can be. I lived in an area where the roads are built to the specification of a grid (american style). This allowed me to have 4 or 5 ways just to go to a shop a few roads away.

Where I live now I could walk 4 or 5 ways to go a supermarket at the end of the main road near me.. Think of the places you go everyday, or often - and think of how many different ways you could get there. Mix them up and use them sparringly.

- If you are going to change your clothes, CHANGE YOUR SHOES TOO.

So many people say "Oh, if people are watching you - or you're worried about CCTV; just wear different coloured clothes underneath or get changes." - thats a good idea in the right situation. It probably works best in crowded areas.. or where you can't see a persons feet - OR LUGGAGE.

People often forget you need somewhere to store the clothes, and it looks obvious if you're the same height, same hair cut, same build and with the same rucksack. So try and go for draw string bags if you must, as they fit easily in a pocket.

The same goes for shoes. If you can't change your shoes, just make sure you wear some common white ones - no shiny silver bits, bright colours or elaborate designs.

- Blending in. Dress to blend in, but don't try to blend in.

Your main objective is to blend in to a crowd with ease, so no "in your face" t-shirts - no matter how funny you think your favourite t-shirts are.. they aren't needed right now. You're Mr."Nobody looks at me"; so don't give them a reason too. Dress like those around you.

Have you ever been to a party and seen someone that barely anybody knows? Even if you don't know many people - you can tell that this guy doesn't know anyone - purely on his body language. Well, thats you. If you TRY and blend in then you wont. Since when does anyone TRY and blend in? You just blend in when you let your mind wander, when you let the atmosphere capture you.. Think about everyday situations when you go shopping, when you get on a train, when you go for a walk... You blend in right? Theres nothing that makes you stand out - as you're just another person. See; you blend in without trying.. so don't try.

- Waste time, its cheap.

Sometimes you'll have to just waste time - make it seem like you're doing nothing in particular. Sit down in starbucks and have a coffee. Sit there and ponder away half an hour...

Or, Sit there and carefully look out around you for anyone watching. Think about your journey - was there anything out of the ordinary? Sometimes you need to sit back and relax, but similarly - you also need time to think about what you're doing, what you've done and whats going on around you. This is the time for it.

- Learn to love public transport.

Public transport is brilliant. Coming from London I have the undeground/tube - and its the dream for anyone who thinks their being followed or watched. Using public transport opens many possibilities up; these range from..

- Getting off a few stops late, getting off just before the doors close and running to the other platform to get a train going back. (Works on the tube where trains are every couple of minutes)
- Getting on a bus and sitting somewhere in which you can watch the whole deck.
- Purchasing a "travelcard" and circling yourself to get to where you want to go
- Basically put, anything that isnt a direct journey - use your imagination

A note for Londoners. If you use the "Oyster Card" system, don't register the card and try to change card every once in a while. Remember every journey you make is logged using this system. Sometimes its better to go for paper travelcards from train stations.

Part 5. Making a successful RV

Sometimes you may have to make a meeting with someone - if so there are a variety of things you need to take into account and put into practice whilst making an RV. We'll start from the very begining...

- Planning
* Avoid secluded spots, go for noisy, and go for busy.
* Aim for somewhere which has multiple exits - and try and take different exits after you've had your "meeting".
* Contrary to what you may believe, pick somewhere you can watch - this will be apparent soon.
* We've discussed travel above, but aim to get to the RV a good hour to 30 mins early.
* Communicate the details of this RV using all of the security methods we talked about in the Personal Security section!

Upon arrival at the RV you need to make sure its appropriate - check for exits and make sure everything looks ok. If you can, give your associate a specific spot to meet you, then arrive somewhere nearby which you can watch from. This allows you 30 minutes+ to ensure that nobody is in the area acting suspiciously - be they leaving items, tampering with anything or just "waiting around".

If you see anything like this call the RV off with your disposable phone, then dispose of the phone. You need to question just how your RV was compromised, and just how trust worthy your associate is now. Either way - You've screwed up big time. Prepare to re-assess your Persec...

- Executing the RV
* 30 - 60 minutes isn't alot of time to be early, and may not be enough - but to wait any longer could make you stand out more than you wish too and could bring more attention upon you.
* Always keep the tone the same no matter what you're discussing; the more relaxed and friendly you look - the better.
* If you're handing over items then you need to be incredibly cautious as it may be very obvious - try and do it discreetly as possible. Even if it means placing your mobile phones on a table or bar (as is common) and picking up the item when you go to leave with your phone. Or, if its larger, have the person place it at your feet whilst you "chat and catch up" and casually pick it up as you leave.

Once you've executed the RV now you need to leave. It may be best to leave at different times again, but at the very least it is probably a good idea to leave via different exits. We've already discussed travel and it should be blatantly obvious that you MUST take a different route back, and that if you have acquired any objects from the RV; don't make a show of them, don't inspect them etc.. that can wait till you're in the safety of your own home.

If the person you're meeting isn't completely trusted then you may wish to try what I call "The mobile RV", or "The Bus Method". I named it this as I had to use it when I met someone who was linked to the people who were after me over the summer. I'll explain it in the form of a story..

I arranged to meet 'A' at the bus stop for the 203, however I couldn't trust her and I knew she *was heavily involved with the people who had made death threats against me. I decided the best course of action was to arrange to meet her at 1200, but ring shortly after saying theres been a delay and for her to wait at the bus stop - "I shall be *walking* along any minute".*

I had grabbed some food at a McDonalds behind the bus stops and watched her arrive. I had scruffy hair, hadn't shaved in a few days and, well - I felt as though I looked homeless. Just another scruffy guy wandering around... I'd arrived at McDonalds a good 30 minutes early and watched her arrive alone - but I couldn't be sure.

I left shortly after 12 and walked down the road 5 minutes to the next bus stop. I grabbed the first bus that would go through her stop and immediately rang her "I'm on the 303, it will be at your bus stop any second now. Wait a second - Stay on the line... Now get on the bus." - by keeping her on the line I ensured I had her full attention and that she wasn't ringing anyone or texting. I acted as though I kept her on the line just so I could say "I can see you now!"; and I guess I did - but I was more worried about seeing her hands and what she was doing with the phone.

When she got on the bus I made sure she was alright, asked her how she was and had a catch-up; at the end we got the same bus back to the same spot and I told her to get off, I wasn't coming with her. I then got off at the next stop, jogged a few streets to another bus stop and started the journey home.

The above story is true, the bus numbers have been changed - but the details aren't. For "A" was the ex which I made a stand for against the guys pushing drugs on her. This explains why I only wanted to ask her how she was.

By using a "mobile RV" you can start your RV anywhere, stop it anywhere, avoid surveillance and have multiple places to go. Definitely worth a think about.

Part 6. Electronic Surveillance Methods

The past few generations have grown up with the image of James Bond - a spy who used all number of gadgets for listening in on his adversaries; whilst the technology he used might be the stuff of fiction - the equipment available today is still heavily advanced and relied upon by law enforcement and private investigators worldwide. You should never underestimate what your opponents could be using against you.

Whilst you can get specific equipment that can scan for electromagnetic radiation, these can often be expensive or ineffective in specific situations. The best ways of trying to "defeat" bugs and similar electronics is to not trust anywhere apart from your own safe home - i.e your house, and to keep your Physical Security as high as you can.

If you must go somewhere which isnt busy and crowded - then think of the book 1984 and go to a secluded field somewhere. However, don't even communicate where you're going to meet beforehand - just meet at the RV then take a roundabout route there.

We should be pretty clear about PC security from the PERSEC information at the begining of this document; however;

- always check the system for physical hardware keyloggers and signal interception devices
- keep your security routine up, and ensure your software is secure - check security websites (securityfocus etc) for details of new vulnerabilities in software you may use
- Encryption, Encryption, Encryption! Encrypt your personal files, Encrypt your emails and Encrypt your IMs.
- Think about shutting down your computer. I often leave mine on standby, but that allows someone to come in and have access to my system whilst there is still data stored in the RAM and applications open - even if it is password protected. (Remember the COFFE app which Police use is mainly used for running on systems which are already booted and have been left running)

Part 7. Tell tale signs of surveillance
Simply put - with the right guys observing you; there will be none. Surveillance should be carried out by highly trained teams, and this is worth bearing in mind. This document is paranoid, and overly so, but its impossible to write such a document without a degree of paranoia. However, you should remember just how much money surveillance takes - atleast professional and high quality surveillance, not wannabe spy Private Investigators who never made it to cop school - or washed up cops who never quite got into the Security Services.

If you have a real set-up watching you then you have a lot to worry about, and no amount of reading can detriment from that. The best ways you can hope to catch surveillance is by having your PERSEC up to an incredibly high level, by having your physical security even higher and your ITSEC/COMSEC at an equal level - with complex IDS systems, and by going beyond the call of duty by doing things such as checking logfiles everynight.

However, with the above in mind - you could bear the following in mind:
- Leave items in specific locations, paperclips attached to the backs of draws... etc
- Install a widget on your system like the mouse-ometer which measures the distance a mouse travels (only useful if your system is left on)
- Tap small peices of thread to places in hard to reach/find places (behind drawers again?)
- Even mess around with party popper style traps - who the hell infiltrates a house to install listening devices and brings a box of party poppers with em to replace ones they use?!
- Make notes of any weird activity by your house, - number plates, times, locations. When out and about try and remember the people you see on your daily commute; look out incase they pop up else where.
- If you want to be brazen about it, in Northern Ireland the IRA were known to simply stop turn around and shout "I know you're following me."! With professional surveillance this really shouldn't affect them at all however.

I hope I have given you a little food for thought about your own security, and about your everyday routine. I should hope none of us needs such a document, but I did find it quite entertaining to write and it did get me asking questions that I've never pondered before. I tried not to make it sound like some "Andy McNab" book, however I fear that boat sailed long ago!

I leave you with one of the most overused lines there is, however - its one that is very true...
[i]"Just because you're paranoid, doesn't mean they're not out to get you".