BRIEFING ON PERSONAL SECURITY, SAFETY & SURVEILLANCE

Contents

1. PERSONAL SECURITY and SAFETY

This section contains advice on precautionary measures that should be taken by all members in order to prevent personal attack, avoid surveillance and protect information in their possession. The precautions needed to be taken by any individual will depend greatly on the assessed threat to that individual. This can be ascertained by taking into consideration such things as position in the Movement, profile, work tasks, contacts, enemy threats and so forth.

Whatever the case, it is impossible for anyone to take all the measures mentioned here or to remain on 'red alert' for twenty-four hours a day. Precautions have to be geared to the possibility of attack or the likelihood of surveillance. For example, most people are relatively vulnerable when entering or leaving their homes, approaching their work places, or at other times when their movements can be anticipated. It is at such times that a high degree of alertness is required.

Vulnerability means openness to successful attack. It is therefore important to learn to recognise a vulnerable situation when it presents itself, and although in practice you may not always be able to avoid it, you should always be prepared to meet it. In this way you, and those around you, will never be taken entirely by surprise.

General

Alertness and vigilance are our primary defences against enemy attack. A person who is awake and observant is less likely to fall victim to enemy machinations than someone who is oblivious to their surroundings and wrapped up in their own existence. Being alert is not just a matter of keeping our wits about us but of keeping a balanced state of mind. Paranoid imaginings that the enemy lurks behind every bush and knows our every move can be as dangerous as heedlessness.

Everyone should at least observe these most general precautions; those who feel they are more at risk should read on:

1. Be alert to suspicious or unaccountable conduct by persons around you or in the vicinity of your home or place of work.

2. Be sensitive to areas of threat or controversy arising from your normal activities or personal circumstances and inform those of your comrades, family and friends who should be aware of the situation.

3. Remember that an attack will only succeed if you are caught unawares. A potential attacker who can see that you and your family, friends and comrades are on guard will be forced to stop and think, however briefly, thereby increasing your chances of taking evasive action or summoning assistance.

4. Summon assistance at the first sign that something unusual has happened or is about to happen. Call for help or sound an alarm. If you are unable to do this for yourself, your family, friends and comrades should be prepared to raise the alarm on their own initiative at the first sign that anything is amiss.

5. Raising an alarm or displaying firmness can of themselves effectively deter potential attackers from continuing their attack.

6. Those close to you may at any time feature in the plans of potential attackers and in general these measures should be regarded as equally applicable to them.

7. Knowledge of your movements and activities should be strictly limited to yourself and those who need to know. The enemy can only work out plans of attack if they can predict your moves.

8. Keep yourself in a fit state of mind to enable you to respond quickly to threatening situations. Drunkenness and inward thinking can cost lives.

Routine

Routine and predictability are our greatest enemies - they enable hostile parties to anticipate our next moves. Always ask yourself: 'Am I following a set routine?'; 'Can anyone predict what I am going to do next?'

1. Avoid establishing observable patterns of behaviour which would enable the enemy to predict your future movements, construct a plan around them, intercept you in conditions unfavourable to you and isolate you from effective assistance.

2. Do not regularly use the same eating and drinking places where people might readily expect to find you.

3. Do not regularly use the same hotels and shops, places of entertainment, recreation and study etc.

4. Do not regularly meet people in the same places or at the same times.

5. Avoid using the same routes to and from places that you regularly visit, such as work and friends.

6. Do not regularly catch buses from the same stop; trains from the same station. Similarly, do not regularly get off buses and trains at the same stops or stations.

7. Try not to regularly use the same bus routes or train lines. You can often get to the same place by using other routes and lines. It might require more effort or take longer, but it's worth it.

MOVEMENT, TRAVEL AND TRANSPORT

General:

1. Never disclose details of your movements to anyone to whom it is not essential that you do so.

2. Whenever you are going somewhere for any length of time make sure that someone responsible at home or your work knows:

a. where you are going;

b. whom you are going to see;

c. how and by which route you will travel;

d. when you are due to arrive;

e. when you are due to return.

AND they should know what to do if something should go wrong.

3. Never make public your travel arrangements. Try not to announce your travel plans over the phone or in letters. When making bookings be sure that no one overhears you, or ask for a destination which is closer to or beyond your actual one.

4. If the risk warrants it, make advance reservations for travel and accommodation in a different name.

5. Always change your routes and times of departure and arrival when making regular journeys.

6. Make a habit of checking the road or area in front of your home or place of work before leaving to see if there are any suspicious persons or strange vehicles in the vicinity. To make this easier, become familiar with your environment and try to memorise what vehicles are normally parked outside the places where you live and work.

7. If possible, travel in company - especially at night.

8. Make a habit of checking that everything appears normal each time you begin and end a journey. Ask yourself: 'Is there anything to suggest that something has changed or that the enemy has taken control during my absence?'

9. Endeavour to be as inconspicuous as possible when travelling in public. Do not wear bright clothing; bags and hats also help tails and attackers to keep on your track.

10. If you are carrying something valuable do not let it out of your grip. Briefcases may be secured to your wrist with a strap or chain; straps of bags should be placed over your head and not just over a shoulder. Let bags hang in front of you but still be careful of pickpockets in crowded situations. Do not use open bags or baskets: make it difficult for thieves to remove important objects.

11. Very important documents and large quantities of money should not be carried in a case or bag. Place them in an inside pocket or conceal them under your clothes where they cannot fall out.

Walking:

1. Always walk with your head up and scan repeatedly with your eyes from the distance towards yourself. Your natural focal point should be the distance, not your feet. Do not daydream; concentrate and remain alert.

2. In countries where cars drive the left, walk on the right-hand side of the road. This allows you to see approaching cars and it makes it more difficult for a car following you to intercept you, as it has to cut across the oncoming traffic.

3. Walk near the kerb or in the middle of the road when it is dark. Keep well away from poorly lit areas, shrubbery, dark doorways or other places of concealment.

4. Avoid short cuts through vacant lots, deserted parks and unlit alleys. Always try to walk where you, and an assailant, would be seen by members of the public.

5. Avoid situations without escape routes; choose routes which offer obvious and multiple paths of flight.

6. Always remember that there is as much space behind you as in front of you. Try to remain aware of what is going on behind as much as in front.

7. Never walk from one place to another along the most direct and obvious route. Walking in an unpredictable way makes it difficult for a pursuing attacker or tail to guess your next moves.

8. Never read anything while walking; avoid animated conversations if walking with someone.

9. Never accept lifts from strangers.

Private transport:

1. Have your rear-view mirrors well adjusted and clean - AND USE THEM.

2. Keep your vehicle in good working order; keep it clean and tidy inside. Remove all articles that could be booby-trapped.

3. If you have a garage use it at all times. Ensure that the garage has a good lock and that other entry points are secure.

4. If you park your car outside your home try to park it in a position in which it can be seen from your house or where it will be in view of neighbours or passers-by.

5. Try not to park your car for long periods in places where the enemy would have the opportunity to tamper with it or booby-trap it without anyone seeing.

6. Ensure that your car is locked and that the windows are up whenever you park. Do not leave valuables in view: put them in the boot.

7. If you suspect a tail, make certain by circulating a block, driving in an erratic way or doing something irrational or 'illegal' like placing yourself in the wrong lane or going through a red traffic light. (For more information on protection of private transport see Section 4 - Car bombs.)

Public transport:

1. When using buses and trains, always seat yourself in a position where you have a good view of other passengers getting on and off.

2. Try not to travel when it is very late or early. Waiting on deserted platforms or in dark streets can be dangerous.

3. When travelling by train avoid empty carriages and compartments.

4. If you have important luggage always try to keep it with you - and keep your eye on it. If it is too large to have with you then sit or stand near it so that you can keep it in view all the time. If you have to surrender your luggage make sure that it is well locked and identifiable. Before opening it on return make sure that it has not been tampered with.

5. If travelling by bus and you suspect that you are being tailed, get off beyond your destination and walk back. If the suspected tail gets off with you you can take evasive action or avoid going to the destination; if not, the tail will get off at the next stop and walk back toward your stop, by which time you will be well away. If you had got off before your destination you would be walking in the direction of the next stop and might bump into the tail.

6. If travelling by train and you suspect that you are being tailed get onto a train going in the opposite direction and then cross over at the next station; or go beyond your destination and catch a train back. If the suspected tail does the same it will be a give-away.

7. When using taxis announce your destination after you have entered it. If this is not possible then ask for an incorrect destination and then 'change your mind' when you are inside.

8. Do not phone for a taxi from your home: the enemy could be eavesdropping and send their own 'taxi'. Do not give the correct name when phoning for a taxi and do not give the exact destination.

9. If your destination is secret do not get a taxi to drop you directly outside the place. Get out some distance away and then walk to your destination, keeping an eye out for tails.

2. HOUSEHOLD SECURITY

For most of us we are at our most vulnerable when approaching or leaving our homes. This does not mean, however, that when we are inside our homes we are safe. The enemy knows that our homes are the one place where they will most definitely find us, at one time or another, and that when we are at home we are likely to be off our guard. Our homes may also contain information and

equipment that is of interest to the enemy and which could jeopardise the safety of our comrades should it fall into their hands.

Physical aspects:

1. Fit mortise dead-locks to all outer doors. Exterior doors should be of sturdy construction but make sure that they are fitted to equally sturdy door frames. Glazed doors should be fitted with burglar bars and obscured with blinds or curtains.

2. Know where all keys for your outer doors are. If you cannot account for them all -

CHANGE THE LOCK.

3. Fit strong door chains to outer doors - AND USE THEM.

4. If your residence is above ground or if you have no view of your front door fit an entry-phone and electrically-operated door release. Alternatively fit an optical viewer to enable you to see visitors before opening.

5. Fit window locks on ground-floor windows and to any upper floors to which access can easily be obtained, especially those hidden from the view of neighbours and passers-by. Any opening windows not normally used can be permanently screwed to the frame.

6. Fit burglar bars to accessible windows that are hidden from the view of neighbours and passers-by.

7. Hang heavy curtains in those rooms most regularly used and see that they are drawn as soon as it gets dark. Use net curtains on windows that allow an easy view into regularly used rooms.

8. Light the approach to your house with exterior lights placed out of reach. See that this lighting is regularly used and maintained.

9. Leave a 'courtesy' light burning in the area of the front door during the hours of darkness.

10. Consider the use of other forms of security lighting for use in emergencies or when suspicion is aroused. Floodlights placed in strategic points make it difficult for would-be assailants to escape without detection or to hide in the shadows.

11. Always have reserve lighting to hand, such as torches, paraffin lamps and candles.

12. Depending on the assessed degree of threat, consider installing a burglar alarm system in your house, and in your garage if you have one. Boundary fencing which makes access to your property difficult for intruders can also be installed. There are boundary alarm systems that can be fitted to warn of penetration.

13. In the absence of peripheral alarm systems, encourage the growth of trees and hedges near your boundary which hinder access to your property. Keep fences in good repair. Try to block the view from the street into rooms which are most often used.

14. Remove and trim shrubs near your house, particularly near paths and driveways, to make concealment of attackers and devices difficult.

15. Always keep at least one approved fire extinguisher in an easily accessible place.

16. Ensure that there is an easily accessible fire escape, about which your family should know and which should be obvious to visitors.

17. Fit a doorbell if you do not have one and make sure that it is working at all times.

Practical aspects:

1. Never answer the door automatically - always check who is there first. Demand to know who it is before opening, or look through a window if you have a view of the door.

2. If you have an answer-phone do not press the door release if you do not know the person or recognise the voice. Even if you know the name, do not press the release button until you are certain that the caller really is who she/he says she/he is.

3. Do not open a door if at all suspicious of the caller. Demand identity cards from anyone who needs access to your home, such as meter readers or workpeople, and watch them while they do their work.

4. Encourage friends, relatives and comrades to inform you of intended visits.

5. Treat late callers, whether known or unknown, with great suspicion.

6. Use the door chain if one is fitted, but always prepare yourself for an intruder.

7. Never leave a key under the doormat, in the mail-box or other obvious place.

8. Know exactly how many keys you have for your house and know where they are or who has them at all times. Do not issue spare keys to too many people or to people you do not know well.

9. Never announce on the phone or write in a letter where you might leave a key, even if the hiding place is a good one.

10. Never leave keys with neighbours unless you know that you can trust them completely.

11. Never leave keys with workpeople who might be working on your home when you go out. Never leave your home while workpeople are working on your home - they may be enemy agents.

12. Never leave your keys in a position where someone could steal or take an impression of them, such as in the pocket of a coat you might hang up in a changing room or restaurant.

13. If your keys are stolen or if you lose them change the locks of outer doors immediately.

14. Make a safety check each night before retiring to ensure that all external doors and windows are locked.

15. Always lock all external doors and windows before you leave the house, even if you are only going out for a few minutes. Include accessible upstairs windows.

16. Always leave a light burning in a front room when you are out at night. Time switches can be fitted to turn lights on and off at random or certain times.

17. Never leave a garage door open when you go out in a car: it suggests the house may be empty and the garage may contain tools useful to someone trying to gain access.

18. When your house will be unoccupied for any length of time try not to allow this to become public knowledge. Best is to have a trusted friend or relative occupy it while you are away.

19. Before leaving your house unoccupied for any length of time make sure that all regular deliveries are cancelled: their continued arrival will signal that the house is unoccupied. Get a trusted friend or neighbour to check your premises daily and to remove any signs that would indicate that it is unoccupied.

Sensitive materials in our homes:

1. Keep your home tidy so that sensitive materials cannot get lost under junk.

2. Keep all sensitive materials under lock and key - preferably in lockable filing cabinets or in a safe. But remember, the first thing an intruder will look for is a keep that is obviously intended to prevent theft. Ideally make or have made a secret compartment that will hold your most sensitive materials. A thief who raids a locked filing cabinet or safe might believe that he or she has found your most important documents or objects and look no further.

3. When working with sensitive materials take out of your compartment the minimum that you need to get on with the job. Situations always arise where an unexpected visitor arrives or you have to leave suddenly. Never leave out of your compartment anything that you would normally keep in it, even if you go out just for a few minutes.

4. If you go away for any length of time leave some sign in your compartment or in the room where it is located to indicate if it has been opened and/or gone through.

5. Regularly go through your sensitive materials and ask yourself: 'Do I really need this?' Keep only what you really need to carry out your work.

6. Do not discard in a bin sensitive materials that you no longer want - the enemy can find them there. Destroy completely materials that you no longer need. Documents can either be burnt or flushed down a toilet, other materials should be burnt or buried. When burning make sure that your fire is hot so that all traces are destroyed; before flushing papers down a toilet saturate them with water and tear them into shreds.

7. Ultra-sensitive information, such as names and addresses, should ideally be kept separate from your main store of sensitive materials. Preferably get someone you trust but who is not connected with your work to keep them. Consider keeping very important information on a computer and/or encrypting it.

8. Never take with you more sensitive material than you will need; check each time you return that everything you no longer need is returned to the compartment or safe.

Children:

Our children might feature in the plans of attackers but of more importance is the fact that without proper discipline they might unwittingly endanger others.

1. At all times keep young children within sight or earshot, or place them in the care of responsible and trustworthy adults.

2. Use only baby-sitters in whom you have complete trust. They should be instructed what to say should the phone ring or if someone should come to the door.

3. Never allow young children to travel to school, friends or other places unaccompanied by an adult.

4. Instruct your children to tell you where and with whom they will be when away from home.

5. Warn your children, of all ages, not to speak to or accept lifts from strangers. The enemy might attempt to acquire information about you through your children.

6. Instruct children never to admit strangers to your home.

7. Discourage your children from answering doors and forbid them to do so during the hours of darkness.

8. Do not allow younger members of your family to open your mail.

9. Forbid younger children from answering the phone as they may unintentionally give out information which may be detrimental to you. Older children must be instructed not to talk about you.

10. Do not discuss with your children or in their presence matters about which they should not or do not need to know. However, excessive secrecy can lead to curiosity and interference with your affairs.

3. SURVEILLANCE

Many of us believe ourselves to be under surveillance. While undoubtedly some of us are, it is important not to allow ourselves to suffer from a persecution complex - believing that our every word and move is the object of enemy attention. If we do we will put the brakes on our activity and nothing will get done: the enemy has achieved its objective.

To keep someone under permanent surveillance is a time- consuming and labour-intensive business. To do the job properly the enemy has to allocate a team of people who have to be equipped with vehicles, radios and the other paraphernalia of surveillance and eavesdropping. Not only that, there have to be people to listen to, transcribe and interpret all intercepted conversations.

Telephones

The telephone is a service provided by the state and as such it gives the providing authority a direct listening channel into our homes and places of work. There is little that we can do to prevent it being used to eavesdrop on our private conversations and for this reason our best defence against it is not a technical but a political one.

There are three basic ways that the telephone can be used to eavesdrop:

1. it can be used to monitor actual two-way telephone conversations;

2. it can be used to monitor non-telephonic conversations in a room or building;

3. it can be used as a power source to run other electronic eavesdropping devices.

Telephone taps are either official or unofficial. The former are those undertaken by the controlling authority and have to be approved by the government where the tapping is taking place. The latter are those undertaken by anyone who wishes to listen to the conversations of another without official approval. In the case of our membership there may be some official taps in place but it is far more probable that most taps will be unofficial - that is, taps carried out by our main enemy in environments which they do not control. This is not to say that there is no collaboration between the authorities in the countries in which our members reside, and our real enemy.

1. Telephone conversations:

There are a multitude of ways that a telephone can be bugged. Conversations can be tapped at any point from the telephone handpiece (receiver) all the way to the telephone exchange. The tapped conversation may in addition be relayed by a number of different methods or be recorded directly onto tape.

Starting from the handpiece, the microphone in the mouthpiece can be replaced by a radio microphone of exactly the same appearance as the original one. This will transmit both sides of a telephone conversation to a radio receiver a short distance away. A recording can be made of the received signal.

Various transmitting devices can be fitted inside the body of the phone, in the wall-socket and inside junction boxes. Similar transmitting devices can be fitted to the line at any point up to the exchange. Some of these can be exceedingly small but then they are exceedingly weak. Most are powered by the current in the phone line so do not need constant replacing of batteries. Certain short-life devices are powered by their own batteries but these would only be used on one-off occasions which the enemy would want to monitor or where an enemy agent can easily gain access to the device.

The best telephone monitoring devices are those which are hard-wired to the line. The tapping usually takes place at a junction box where a spare pair of wires in the eavesdropper's line (this may be a neighbour or someone in an office in the same building) is attached to your pair. This leads your signal off to wherever a tape recorder can safely be located. Each time you pick up your handpiece the recorder will be activated and every word of your conversation will be recorded. When there is an official tap on your line it is done in this way except that the tapping is done at a special station which has a direct line to your local exchange.

2. Non-telephone conversations:

There are a number of ways that a telephone can be kept 'alive' or 'off-hook' so that conversations picked up with a microphone can be be fed into the telephone line. A microphone can be connected to the line at any point (the wires to the microphone can be any length so the microphone itself need not necessarily be near the line) or the phone's own microphone can be used to pick up conversations in a room. This means that conversations in a room can be listened to from anywhere in the world, not just along the connection to the local exchange.

3. The telephone as a power source:

As there is a voltage in the phone line it can be used in the same way as the mains to power eavesdropping devices. Thus all manner of bugging devices can be attached to the phone line to transmit both telephone conversations and ordinary conversations in the room where the microphone of the device is located.

What to do about it:

The best advice that can be given about preventing telephone eavesdropping is: DON'T USE IT. The telephone is a very dangerous instrument and not a few of our most important secrets have got into the hands of the enemy this way.

We have to be very strict with ourselves about using the telephone. Over many years we have grown dependent on it and in some situations it requires great effort to convey messages by other methods. If you have no choice but to use the telephone then at least cultivate a correct attitude about using it and take elementary precautions to disguise information:

1. Always assume that there are the three parties involved in every phone call you make: you, the person you have called and the enemy.

2. Before making an important phone call always ask yourself: 'Is there not another way that I can get this information to the other person?' Don't opt for the telephone just because it's 'too much bother' to do it another way. Better later but safe.

3. Always use an agreed code language when talking about important matters. This should also contain a method of indicating dates and times. However, it must be remembered that to an eavesdropper it is obvious when a code is being used so don't believe that you are safe when you use one. The code itself indicates that you have something important to hide.

4. Keep important calls as short as possible. The less you say the better.

5. As far as possible try to use public telephones for making important calls. But do not always use the same callbox - that could be as bad as using your own phone! Also, there is not much point in using a public phone if you suspect that the other person's phone might also be tapped.

6. Always ask yourself after you have made a call: 'Did I say anything that could be of use to the enemy? Did I say anything that could be added to what I have said before?'

It is almost impossible to be certain that your phone is not tapped as the tap could be an official one. However, it may be possible to detect unofficial taps and there are a number of measures that can be taken to defeat them and other forms of bugging using the phone line.

1. Always remove the telephone instrument from the room in which you are having an important conversation. However, this does not mean that you are safe as a separate microphone attached to the phone line could still be picking up and relaying your conversations.

2. If you suspect a bug inside the body of your phone then open it and have a look. There should be nothing inside apart from what is obviously attached to the circuit board. If you are still uncertain then buy a new phone - they are very cheap these days!

3. Open the phone socket and check for microphones and bugs. There should either be nothing or if there is a small circuit board then no more than one or two small components obviously fixed to it.

4. Follow your phone line all the way to the junction box from where it feeds to the street. There should be nothing attached to it, no lines branching off it and at the junction box there should be no more than a pair of wires connected to the street side of the connector to which your pair are attached. If there are connections it could indicate that your line is taking a deviation to a recording post nearby.

5. Whenever you get a wrong number always lift the receiver a few seconds after you have put it down. This will turn off 'keep-alive' bugs which are activated when the false caller calls.

6. If you are still worried about phone bugs then take the precautions mentioned in the next section on 'bugs'.

'BUGS'

The term 'bug' is usually used to refer to small radio microphones, but these are not the only type. There are a great variety of radio bugs but most work by capturing a conversation with a microphone and then relaying it by air to a receiver situated some distance away. It is important to realise that for every bug there must be a receiver, as well as either someone listening to the receiver with a pair of earphones or a tape recorder recording the received signal. Thus it is impossible for there to be a bug in every room of all our houses, or even every room of the house of someone important.

Bugs are either powered by available permanent power sources such as the mains or the phone line, or by battery. This has a bearing on the nature of the bug. Mains-powered bugs can be placed or disguised in permanent fixtures while battery-powered bugs have to be accessible for battery replacement. Thus mains-powered bugs are usually used where the surveillance is intended to be permanent or long-term and battery-powered bugs where the surveillance is one-off or short-term. Mains-powered bugs are generally more powerful as they have an endless and large source of power. They may be disguised in sockets, switches, adaptors, fixtures, lamps, appliances or any other device that plugs into or can be connected to the mains.

The mains itself can be bugged in much the same way as the phone line and anyone connected to the same circuit can listen to a conversation in a bugged room by connecting their receiving unit to the circuit. The captured signal is carried through the mains wires without being broadcast.

Battery-powered bugs are usually planted out of sight in a room where it is known that an important conversation is to take place shortly before the event. Unless the planters of the bug have someone who can without suspicion gain access to the bug to service it (i.e. a 'mole' or 'plant'), the bug is discarded or retrieved after the event.

What to do about bugs:

The most important defence against bugs is adopting a correct attitude to them. There cannot be bugs everywhere as each one means that someone has to listen to and transcribe everything that is said in its presence. This means tying down a vast workforce and the use of large quantities of expensive surveillance equipment for possibly little gain.

If there are not bugs everywhere then there are bugs where it is going to be profitable for the enemy to plant them. Our defence is to not allow situations to arise where it becomes profitable for the enemy to do this. This means being very disciplined about where important meetings and

conversations take place. Meetings held regularly in easily accessible places mean bugged meetings.

1. Never announce out load at important meetings when and where your next meeting is to be held. If the meeting is bugged the enemy will know when and where to place the next bug.

2. Never talk on the phone about the times and places of important meetings. You could give the enemy warning.

3. Never send in the post notification of important meetings. You will give the enemy advance notice.

4. Never hold important meetings regularly in the same place. A bug will be planted as a permanent fixture.

If you suspect that a room in which you intend to have a meeting is bugged there is no substitute for a good physical search for the bug. While it is possible to purchase special instruments that can detect the presence of bugs, these can never discover all known types and thus give a false sense of security. In addition an improper understanding of how bugs work will make it difficult to interpret what the bug detector is saying.

1. Open all wall sockets and switches to look for hidden bugs.

2. Pull forward all furniture against the wall and look behind it, under it, under any shelves and in compartments etc.

3. Inspect any immovable fixtures. Especially look under low shelves and behind heaters etc.

4. Investigate any unaccountable wires running through the room. Every wire must have a source and ending; otherwise remove it.

5. Look behind any pictures or other fixtures to the walls. In addition inspect skirtings and rails for holes which might conceal microphones.

6. Inspect all items in the room that could conceal a bug. Bugs can be concealed in virtually anything - suppliers sell them hidden in light bulbs, calculators, cigarette lighters, ornaments, lamps, adaptors, pens, cigarette holders, etc.

Even after a physical search has been conducted and nothing found, a participant in the meeting could bring a bug into the room. Perhaps consideration should be given to physical searches of people and items in their possession such as briefcases and bags. In addition the following practices should always be adopted even if nothing is revealed through a search:

1. Do not hold important meetings in rooms where the enemy might expect you to meet. For instance, in private residences do not meet in living rooms; meet in bedrooms, the bathroom, the kitchen, outrooms or even the toilet.

2. Shift furniture against the outer walls of rooms in which you meet and then sit in a huddle in the empty part of the room.

3. Place a sound source behind yourselves such that it is between you and suspected bugs in the furniture and/or in the peripheral parts of the room (eg. walls). Best is to use pre-recorded

speech and to play several recordings in different parts of the room. Music does not effectively obliterate speech and can in any case be filtered off from a recording because it is usually of a higher frequency than speech. Direct speech from the radio and TV can be recorded by the enemy and used to eliminate the same from a recording they make of your meeting. Do not have the volume of the sound source too loud as this will force you to raise your voices.

4. As far as possible write the most important parts of your conversation and show it to the other participants. Never say out aloud the names of people who might be compromised by your doing so or mention addresses, important dates, projects etc.

MICROPHONES:

Microphones are used in situations where it is not practical to use bugs, such as outdoors. Microphones are also used in situations which are controlled by the enemy (e.g.. hotels) and where the enemy can get close access (e.g.. next door).

Directional microphones and parabolic reflectors are used outdoors to pick up conversations from afar. The defence against them is to have a loud source of noise in the background (e.g.. traffic) or to keep changing your position or direction of movement.

There are many kinds of specialised microphones for use in special situations. For instance there are 'keyhole' microphones for listening through cracks and small holes in walls of adjacent rooms, 'contact' microphones for listening through thin partitions and windows, 'laser' microphones for picking up the vibrations of speech on window panes. The defence against microphones generally are the same as those for bugs.

4. CAR BOMBS

The booby-trapping of vehicles is a method of attacking our members which has been resorted to by our enemies in the past and could still be used in the future. It is a particularly pernicious method of attack because car-bombs are difficult to detect and they can be effective in achieving their objective.

Types of car bombs:

The various types of car bombs are distinguished by the ways that they are detonated. There is an almost infinite variety of methods of detonation due to the complexity of vehicles and the range of physical actions and processes that take place when a vehicle is in operation. Bombs can be rigged to function in a vehicle by pressure, pressure-release, pull, push, tilt, acceleration, braking, motion, velocity, electrical, chemical, thermal and barometric activating systems. In addition, a bomb can be placed in a vehicle and detonated by various detonating systems independent of the vehicle. A timing device set to fire the bomb at a time when it is known that the target person will be in or near the vehicle can just as well be used. Remote firing methods such as concealed wires and radio control can also be used.

The table at the end of this section indicates some of the places where bombs could be located and the methods that would be used to detonate them. There are four basic areas where a bomb can be placed in a vehicle:

a. the engine compartment;
b. the outer bodywork, including the underneath of the vehicle;
c. the passenger compartment;

d. the boot.

What should be borne in mind, however, is that a car-bomb consists of two essential components - an explosive charge and a triggering mechanism - and that these are not necessarily together in one of these four areas.

A. Engine compartment:

Bombs placed in the engine compartment are usually wired to the ignition coil or starter so that they explode as soon as the ignition key is turned. However, they could be wired to any electrical point and be detonated by any switching action of the bomb-placer's choice. For instance, the bomb could be detonated by switching on the lights, pressing the hooter, turning on the wipers, pressing the windscreen washer, pressing the brakes, turning on the radio etc.

Apart from direct connection to the car's electrical circuitry, a bomb can be detonated by other processes in the engine compartment. A bomb could be attached to the side of the engine block or to the exhaust manifold and with a thermal switch be made to explode when the engine reaches a certain temperature. Virtually any moving part in the engine compartment can be booby-trapped. The bonnet itself can be fitted with a pressure-release switch to cause a bomb to explode when it is lifted up. A bomb could even be made to explode when the accelerator or clutch is depressed. To achieve maximum effectiveness bombs placed in the engine compartment are usually placed against the back wall just above the driver's or front passenger's legs or inside the hump which contains the gearbox or the gear linkages.

B. Outer bodywork:

Bombs attached to the outer bodywork may be triggered by any moving part which could be made to close a switch. For instance, switches connected to the suspension may either be closed by compression or pressure release. Vehicles which are front-engined but rear wheel driven have a drive-shaft to which a pull device may be connected. A switch attached to the steering could be rigged to close when the steering is turned one way or another or only when a sharp corner is negotiated. A thermal switch can be attached to the exhaust pipe and set to explode a bomb when it reaches a certain temperature.

Bombs can be attached to any part of the outer bodywork, under wheel arches and under the floor pan of the car. Most likely places will be just below seats and inside wheel arches nearest to where the target passenger or driver is likely to sit. Such bombs will most likely be held in place by magnets. Remote controlled devices will need to be attached to fairly exposed places as wires or radio waves will need to be able to reach them. Such a bomb might even be placed on the ground under a vehicle.

C. Passenger compartment:

Inside the passenger compartment a bomb could be triggered by a pressure switch or mat placed under a seat, seat cover or a carpet. Switches can be connected to any moving part in the interior, such as the glove box, cigarette-lighter, ashtray, door and window handles, mirror, switches, dials, pedals and so on. Common hiding places for the explosive charge inside vehicles are under seats, behind the dashboard, in vents and in door panels. An incendiary bomb set to explode when the car is travelling can cause a serious accident when the interior fills with fire and smoke.

D. Boot:

In the boot a triggering switch can be attached to the boot lid or any object in the boot such as the spare tyre or jack. A favourite mounting spot for bombs is on or near the petrol tank. A simple incendiary bomb mounted on or near a petrol line can start a fire or even cause an explosion of the tank without the need for explosives.

A car bomb need not in fact even be mounted in a vehicle. One could be placed near a vehicle, such as in a garage, and be triggered by the car when the ignition key is turned or when the car moves off or onto a pressure switch.

Any movement of the vehicle can be used to trigger a bomb. Vibration switches will fire a bomb as soon as a door is opened or closed; less sensitive ones when the car hits a pothole. An anemometer (wind-speed measuring meter) can be rigged to operate a switch when the vehicle reaches a certain speed. Tilt switches can be made to operate when a corner is taken or when the vehicle is driven up or down an incline. Accelerometers or simple pendulum switches can be rigged to close a switch when the car accelerates or brakes. A barometer can be wired to close a switch when a certain height above sea level is reached, thermostat switches to operate when a certain temperature is reached and even a mileometer set to explode after a certain distance is travelled.

How to protect against car bombs

It is more important to develop a correct attitude toward car bombs than to know all the possible locations where they can be placed and all the possible methods by which they may be triggered. This means being constantly vigilant and trying never to leave an opportunity for the enemy to plant a bomb.

In view of the multitude of places where a bomb can be planted and the hundreds of methods by which they can be triggered, conducting regular vehicle searches can be unproductive, and in itself a dangerous practice. Before placing a bomb the enemy will have done some reconnaissance and if it was noticed that a search is conducted each day it would be simple to booby-trap some part of the car, such as the boot or bonnet, which would cause a bomb to explode while the search is being conducted. A bomb triggered by a vibration switch will be fired as soon as anything is opened or bumped.

A thorough vehicle search can take hours if done properly. Every moving part of the car has to be tested by remote methods and every possible location has to be exposed. This means the doors, bonnet, boot lid, cubby hole etc. have to be opened; door panels, seats, carpets, hub caps, and so on removed. Even then there can be no certainty that every possible location has been exposed. A bomb can be secreted in a number of places where it would not be revealed except by careful probing. One such place is in the petrol tank, another is inside the engine.

How then can we protect against car-bombs? The best possible advice is to ensure that the vehicle is securely locked in a garage when not in use and guarded at all other times. It can take only a matter of seconds to attach an explosive device such as a magnetic limpet mine. Since not everyone has a garage and can have their car guarded while not in use, this is unrealistic for many people. However, everyone can take a number of steps which will reduce the risks of bomb placement or at least reduce the number of possible locations where a bomb can be placed.

Always ensure that when the vehicle is left standing the doors are locked and the windows properly closed. While it is possible to pick locks, this can be a difficult and time-consuming task. Locking will reduce the chances of the passenger compartment being used as a location for the placing of a bomb. The same applies to the boot. The bonnet of most vehicles can be opened from the outside despite the fact that most vehicles have a release catch inside the passenger compartment. To make

it more difficult to use the engine compartment as a bomb placement area, bonnet locks should be fitted. This is important also for the reason that it will make access to the vehicle's electrics more difficult. On most vehicles the engine compartment can be reached from underneath, but if panels are fitted under the engine this area will be removed from the bomb-placer's options.

Always ensure that the petrol filler cap is locked or fit a lockable cap if the vehicle does not have one. If the bottom of the vehicle is smooth it might be possible to fit wooden panels to prevent the attachment of magnetic devices. A number of other steps like this can be taken to eliminate areas where a bomb could be placed, but these differ from vehicle to vehicle. Possible locations should be sought out and filled with something or removed altogether if they are not vital to the functioning of the vehicle.

The fitting of a vehicle burglar alarm is another valuable safety measure, but if you do so do not advertise the fact. An alarm which operates on various areas and not only the passenger compartment is best. And make sure that it is not one which is easily immobilised. Alarms which protect the under surface of a vehicle are also available but these are only reliable if the vehicle is parked in a garage. If the vehicle is kept in a garage it is better to fit the garage with an alarm rather than the vehicle.

Avoid having any internal or external mascots or unnecessary attachments which could be booby-trapped or used to hide or disguise some device. Keep the engine compartment clean and the interior and boot tidy and uncluttered so that a strange object will be spotted immediately. It is possible for any object, such as an aerosol can or tin of polish, to be removed and replaced with a booby-trapped replica. Become familiar with the layout of the engine compartment and other areas of the vehicle so that a device will be noticed immediately. Ignorance here can be very dangerous. If you do carry out a search then do so very carefully. First of all, view your vehicle from the side and at a distance to see if there are any objects obviously protruding from the bottom or placed on the ground below it. Without touching the vehicle look inside the wheel arches (carry a small torch with you if necessary) and look more closely at the under surface below the passenger compartment. Open the vehicle from the passenger's side and release the bonnet catch. Lift the bonnet and scan the interior of the engine compartment, especially the rear side. In the passenger compartment look under seats and under the dashboard, and in the boot look in the spare wheel well. But remember, if you do not see what obviously appears to be an explosive device during a cursory search like this it does not mean that your vehicle is not booby-trapped. However, doing this is better than not doing it.

It must be repeated that there is no substitute for vigilance and having the correct attitude toward vehicle bombs. Burglar alarms can give a false sense of security and letting one's guard drop can be disastrous.

WHAT TO LOOK FOR

In the movies the star always discovers the bomb because the villain has been shoddy and left wires sticking out or bits of wire under the car. This is unlikely to happen in the real world. Our enemy is sophisticated and has access to all the latest techniques of bomb-making. It is unlikely that the bomber will construct the bomb at the vehicle - this is too dangerous and the chances of being observed are greatly increased. The enemy will know what kind of car the target individual owns or uses and a bomb will be prepared beforehand for that specific make of vehicle. This will enable the placer to attach the bomb quickly and without any danger to him or herself. If efforts have been taken to reduce the number of placement areas the enemy's plans may be thwarted.

There are many misconceptions about the appearance of car-bombs. More likely than not the bomb will not be half a dozen sticks of dynamite tied together as they are in the cop movies. It is more likely that TNT or plastic explosive will be used and that the bomb will be inside some sort of container complete with its detonating mechanism.

A bomb need only be very small. A 200 gm block of TNT the size of a bar of soap is sufficient to kill someone if placed directly under or near the victim. Common charges are one or two kilograms, but they may be very much bigger if place in the boot or under a seat. Plastic explosive can be moulded into any shape but will probably be placed inside some container which will probably also contain the firing mechanism. Plastic can be secreted inside any hollow space in the vehicle. This is why these areas must be eliminated as far as possible.

The most likely locations for the explosive charge will be near where the victim is likely to sit. This means under a seat, in the door nearest the seating position or directly in front of or behind the seat. The bomb could of course be placed anywhere if it is powerful enough. By far the most common locations are on or in external areas which can be reached without needing to open anything, or at the rear of the engine compartment (if the engine is in front).

It is impossible to say exactly what a bomb will look like as there are so many ways of making them, and they can in any case be disguised. Look for wires running to objects in which explosives could have been placed. If the vehicle's own electrics is being used to detonate the bomb one wire will be connected directly to the bodywork or some other metallic part of the vehicle. The other wire will probably lead to the switch or detonating device and then to another wire of the vehicle's electrical circuit. It is probable that bomb wires will be of a different colour to the vehicle's wires or they may just be cleaner. If separate batteries are being used these will probably be sealed inside a container with the explosive or attached by a pair of wires not connected to the vehicle's wiring in any way.

Most vehicles do not have many loose wires in the engine compartment and other places. Wires are usually bound together or are part of a harness. Get to know which are the normally loose wires so that if you see any others they could be connected to a remote timing or triggering component, trip wires or pressure plate.

DISCOVERING AN EXPLOSIVE DEVICE

Should you discover what appears to be an explosive device never attempt to defuse or remove it on your own. If possible call the police; if not possible, call an expert and clear the area.

Do not attempt to disconnect wires or the vehicle's own battery should you see that the bomb is connected to the wiring circuit. The bomb may be fitted with a collapsing-circuit switch which would detonate when disconnected. This is a switch which is held open by the vehicle's own current but which closes when the current is withdrawn.

POSSIBLE LOCATIONS OF VEHICLE BOMBS

A. Engine Compartment:

Location of charge	Triggering method	Firing method
Engine block	Heat switch on exhaust manifold	Electric/chemical
Engine compartment wall	Push/pull switch on suspension	Electric
Engine compartment wall	Wired to coil and ground	Electric
Between gearbox/floor	Wired to starter and ground	Electric

Steering gearbox	Pull switch connected to tie-rod	Electric

B. Passenger compartment:

Glove compartment	Pressure release switch on door	Electric
Under seat	Pull switch attached to door	Electric
Under seat	Pressure switch	Electric/chemical
Under seat	Pressure mat under seat cover	Electric
Under rear seat	Time delay (incendiary)	Electric/chemical
Under dashboard	Pressure mat under carpet	Electric
Behind door panels	Vibration switch	Electric

C. Outer bodywork:

Under floor pan	Vibration or motion switch	Electric
Under floor pan	Anemometer, barometric etc.	Electric
Under floor pan	Pull switch to drive shaft	Electric
Wheel arches	Pull/push switch to suspension	Electric
Above petrol tank	Heat switch attached to exhaust	Electric/chemical
Inside petrol tank	Time delay	Electric/chemical

D. Boot:

Over petrol tank	Time delay	Electric/chemical
Boot	Pull/pressure switch to lid	Electric
Spare wheel well	Pull/pressure switch to wheel	Electric

5. PACKAGE BOMBS

The enemy has for a long time made use of letter and parcel bombs to attack our members, and there is no reason to expect them to cease using this method of eliminating or incapacitating specific members in the future.

Letter and parcel bombs are most likely to be directed at the leadership of our organisation or at identified active members, but this is not their only use. A parcel bomb can be constructed powerfully enough to cause considerable damage if it explodes inside a building.

There are certain stereotyped ideas of how letter and parcel bombs are constructed, look and are used. Armed with only this scanty knowledge we leave ourselves open to deception and hence to all the dangers inherent in these devices. We must constantly remind ourselves that our enemy is powerful and sophisticated and will resort to every devious means to deceive us. New and progressively more ingenious devices will be devised to overcome the known methods for detecting these types of bombs. For this reason it is of the utmost importance that the enemy should not know what precautions we take to protect ourselves from such devices and what steps we take to minimise their effects should one go off. Whatever protective equipment is used should be unknown to all except those authorised to use it; and whatever procedures are used to handle mail and other deliveries should remain absolutely confidential.

Types of parcel and letter bombs

Letter and parcel bombs (from here on called 'package bombs') can take a wide variety of forms, limited only by the bomb-maker's imagination. Package bombs are not necessarily designed to kill. They are often designed to main, injure or simply cause damage to property (by fire or explosion).

Package bombs can be divided into two basic groups:

1. Incendiary or low-explosive bombs

2. Commercial and military high-explosive bombs.

1. INCENDIARY AND LOW-EXPLOSIVE BOMBS:

These bombs have charges which are usually made from easily obtainable chemical powders which are simply mixed together. Examples of such mixtures are gunpowder, various 'black powders', oxidising agents with oil, and 'flash powders'.

1.1 Incendiary bombs:

These are designed to cause injury or damage through a flash or fire rather than by explosion. Virtually all methods of ignition or detonation used for other types of bombs can be used with incendiary bombs, but because they need only a spark, flash or flame to be ignited, some very simple methods of initiation can be used, which make this type of bomb very hard to detect.

1.2 Low-explosive bombs:

Most incendiary mixtures are in fact low explosives. When packed loosely in an envelope or some other weak container, the action of low explosives when ignited is to flash rather than explode. When a low explosive is packed in a container which offers more resistance to the expanding gases liberated by ignition, an explosion occurs. The more rigid the container the more powerful the explosion.

Any ignition method used for an incendiary bomb can be used for a low-explosive bomb. However, because of the need for a low-explosive bomb to have a rigid container, electrical firing mechanisms would probably be preferred as they are more reliable.

Low-explosive bombs can, if they are sufficiently large, be lethal. But because of the quantity of explosive needed to make one powerful enough to kill, their function would probably be to maim the victim. It is not too probable that our enemy would use bombs charged with low explosives as these would be bulky and arouse suspicion. It cannot be ruled out that other cranks in the service of our enemy may use low-explosive bombs. A low explosive can be made by anyone with chemicals which are freely available. They are easy to set off and do not need commercial or military detonators.

2. COMMERCIAL AND MILITARY HIGH EXPLOSIVES

Low explosives are mere mixtures of various separate chemicals, whereas in high explosives the various chemicals out of which they are made are bonded into a unitary compound. Because there are no air spaces between the chemicals they can react immediately with each other. This increases the explosion velocity considerably and accounts for the greater power of high explosives.
Low explosives work by creating large volumes of gases very rapidly. These expanding gases cause the blasting effect of low explosives. To increase the pressures rigid containers are used. High explosives do not work so much by creating hot gases under pressure, but by a powerful shock wave which is created when they explode. For this reason high explosives do not need any container to be effective. There are a number of other differences between low and high explosives, but these need not concern us here. All that needs to be known is that high explosives are much

more powerful and hence more dangerous than low explosives. Only small quantities are required for the same effect.

The difference between commercial and military high explosives is that the former are available to licensed commercial users, whereas military explosives are restricted to military users. Military explosives are generally more powerful and are packaged in ways which make them far more suitable for use in package bombs.

2.1 Commercial high-explosive bombs:

It is not very likely that our enemy would use these types of explosives, despite the fact that they are fairly freely available. The form in which they are supplied does not render them suitable for concealment in small packages. Dynamite comes in paper-covered sticks which are fairly bulky. The explosive can be removed from its paper covering, but since dynamite is rather mud-like it has to be placed inside some other leak-proof container. Nitro-glycerine is a thick oily liquid and is far too unstable to be used on its own. Gelignite also comes in sticks, whereas smokeless powders are used as propellants in gun cartridges.

The various methods of detonation will be dealt with in the next section; suffice it to say that all commercial high explosives need a proper blasting cap (detonator) for initiation. A blasting cap is a short copper or aluminium tube about 40mm long and 8mm in diameter. They come in two types: electrical and non-electrical. Non-electrical caps are set off with a piece of ordinary black-powder safety fuse. This has to be lit with a flame, so they are not likely to be used in package bombs. An electrical blasting cap contains a few grams of high explosive and an electrical bridgewire. When the cap is connected to a battery or some other source of electricity, the bridgewire glows in much the same way as the filament of a bulb. This causes the cap to explode, which in turn detonates the surrounding explosive into which it is placed.

2.2 Military high-explosive bombs:

There is a great variety of military explosives, but the two most common types used in letter and parcel bombs are TNT and plastic explosive.

TNT comes in 200 gm blocks about the size of a bar of soap. It can be cut down to any size that is wanted. TNT is a hard substance and to detonate it a blasting cap has to be inserted inside the block or piece. Usually there is a hole in the side of the block into which the blasting cap fits.

Plastic explosive is by far the most suitable explosive for package bombs. It is like plasticine or putty and can be moulded into any shape. It can be rolled into flat sheets or inserted into any hollow object in order to disguise it. It is one of the most powerful explosives in use, sometimes as much as twice as powerful as TNT for the same weight. Only a small quantity is needed to make a lethal bomb. For instance, 100gm of plastic explosive is sufficient to cut a railway line. A blasting cap which contains 2gm of relatively weak explosive is enough to blow off your hand. A letter containing 20gm of plastic explosive can thus inflict serious injury. A parcel with a few hundred grams means certain death.

HOW THEY WORK

Practically all package bombs are set off by the act of opening them. This need not necessarily be the case, however. A package could be timed to go off after a certain period, even before it is opened, such as at the time when it is due to be delivered. Others which are disguised as a gift, for instance, might be timed to go off some time after they have been opened.

There are hundreds of different ways of making package bombs go off, but this should not intimidate us as most work on the same principle. Often the shape of the package will inform us of the probable method used.

As explained, incendiary and low-explosive bombs do not require detonators to be ignited and may be set off by a spark or flash. They therefore do not need batteries, wires and switches as part of their firing system.

The inside of an ordinary Christmas cracker can be used to initiate a low explosive. The one end of the cracker can be fixed to a smaller envelope and the other end to the inside of a larger envelope. As the smaller envelope is pulled out the flash from the cracker can ignite the explosive. Even a match can be used by having it scrape against a piece of matchbox side as a package is opened or something moved from inside the package.

High explosives need a detonator to be initiated and since the explosion, usually, needs to take place at the precise moment the package is opened, they are fired electrically. The electrical circuits of such bombs are very simple. A battery is connected to the detonator by wires. On one of the wires is a switch. The act of opening the package closes the switch. This completes the circuit and the detonator fires.

Every bomb wired in this fashion also needs some sort of setting or arming mechanism which prevents the bomb-maker from being blown up before the package is closed. This usually takes the form of another switch in the circuit which is open when the firing switch is closed, but which can be closed after the bomb has been sealed or shut or while it is being sealed or shut. Another method is to fit a timing device to the circuit which closes the second switch after the bomb has been dispatched to the target recipient.

Knowledge of this is important because often package bombs have tell-tale signs which are the result of this need to have some form of activating mechanism.

EXAMPLES OF PACKAGE BOMBS

A few examples are mentioned here to give some idea of how package bombs are constructed.

Many package bombs work by the action of removing one object from the inside of another, such as taking a smaller envelope out of a larger one. This action can cause two ends of an electrical circuit to make contact. Sometimes one object inside another simply holds apart a spring-loaded pair of contacts. Imagine for example a clothes peg which has been fitted with metal contacts in its jaws being held apart by a small envelope in a larger one. As the smaller envelope is pulled out the jaws would snap together and contact be made. More sophisticated switches based on this simple idea are common in package bombs.

Another common switch in package bombs is a pressure-release switch. These are spring-loaded switches which are held open by a lid on a container or by the flap of an envelope. As the lid is removed or the flap opened the switch springs out and makes contact.

Very common in book bombs are reed switches. These are very delicate and sensitive switches that are held open by a small magnet. When the magnet is moved away from the switch the switch closes and contact is made. Book bombs have an area hollowed out in the middle of them between the covers. In this hollow the explosive, the battery and the switch are placed. The magnet is fixed to the front cover while the switch is fixed to the back cover. When the book is opened the magnet

moves away from the switch and the switch closes. A hollowed out bundle of magazines or papers could work in the same fashion.

Many other ingenious 'switches' have been and can be used in package bombs. For instance a package could be wrapped in two layers of aluminium foil insulated from each other and then covered in paper. The two ends of the electrical circuit could be attached to each of the layers of foil. As the cover is ripped off the layers of foil would touch and contact be made.

HANDLING PROCEDURES AND DETECTION METHODS

There are several technical means of detecting package bombs but metal detectors, explosives' vapour detectors and X-ray scanners are the most common. Before looking at these in more detail, we must first look at the most important method of all - the COMMON SENSE METHOD. The common sense method requires no equipment at all - it means the development of a correct attitude to the possibility of receiving a package bomb and the establishment of regular procedures for the handling of deliveries of every kind.

Most people during the course of their lives receive hundreds of letters, parcels and deliveries, yet only one of these is enough to blow you to pieces. Thus, our greatest enemy is letting our guard drop by not constantly reminding ourselves that we are enemy targets and that every object we receive might be potentially lethal. The following is a list of DOs and DON'Ts that should be observed by everyone, whether they have technical equipment to assist them or not:

1. DO remind yourself every time you receive an item of post or A DELIVERY OF ANY KIND that it might be dangerous.

2. DO develop procedures for the handling of regular deliveries, such as the post. Separate all items which could not possibly contain anything harmful, such as postcards and very thin letters. If in doubt, hold the letter up to a strong light. Heavier items should be put aside and treated as suspect.

3. DON'T let anyone else know what procedures or methods you use to handle or detect bombs, as the enemy might find out and use this information against you in the future.

4. DO treat as suspect any delivery large enough to contain something dangerous, no matter where it comes from or how it arrives.

5. DO study the address on any postal item before you open it. If possible, make a note of who posted it, when and from where.

6. DON'T consider an item safe because it comes from a known source, because you recognise the handwriting, because it is a regular delivery or because you were expecting it. The enemy can intercept our post and booby-trap it.

7. DON'T stereotype package bombs. They can be any size and shape. A few grams of high explosive can be very harmful and new almost undetectable methods of detonation might be used.

8. DO inspect carefully any suspect item before you open it.

9. DON'T open suspect envelopes before feeling the contents. Do not bend an envelope. Gently move your hand across the side. If you feel a round object a little thinner than a pencil and about 3 - 4 cm long, it could be a detonator. Other hard objects could be batteries and switches.

10. DON'T poke into a package with metal objects as this could cause a short circuit and fire the bomb.

11. DON'T open packages in the way that you are supposed to. The bomb-maker has made certain assumptions about the way you are expected to open a package. If you open it in an unconventional way you may avoid activating the triggering mechanism and you may see that it is booby-trapped. But be careful.

12. DO open packages very carefully, noting how they are sealed. Tight flaps, openings, lids, string or tape might be holding pressure-release switches.

13. DON'T pull smaller envelopes out of larger ones until you are sure they are not attached in some way. If there is any resistance the inner envelope might be booby-trapped.

14. DO always use remote means of opening where possible. Attach a long piece of string to anything that has to be pulled or lifted and pull it from a safe distance.

15. DON'T submerge a suspected bomb in water. Water is a good conductor and might short circuit a switch. The water might also react with the chemicals.

16. DO, where possible, take suspected packages to the police. Where this is not possible, open the package in a safe place by remote methods.

17. DO, where possible, make use of detection equipment, but remember, these are only aids and not infallible. Their use does not let you off taking the aforementioned precautions.

BOMB DETECTION EQUIPMENT

If you acquire any special equipment to detect package and other types of bombs, it must be remembered that such equipment is only an aid and can never replace the common sense approach. It is very easy for expensive and fancy-looking equipment to give us a false sense of security. Every method has its advantages and its shortcomings. Each type of equipment detects certain kinds of bombs better than the other types of equipment, but none are able to detect all types of bombs. There is no infallible piece of equipment.

1. Metal Detectors:

As the name indicates, these can only detect bombs where metal is present. Although this is the case, a metal detector is useless if the bomb is contained in a metal container, such as a tin, or if it is wrapped in foil. Also, if a bomb is placed deep inside, say, a large wooden box, the distance will be too far for the metal detector to register.

Metal detectors are the cheapest form of detection equipment available. Simple metal detectors used by builders to locate pipes and wires in walls are perfectly adequate for the purpose. Metal detectors are simply swept over the surface of suspect items and give off a tone or a light comes on when they are brought near metal. Although most of them are sensitive enough to pick up staples and paper-clips, this is not a shortcoming because one soon learns to identify these things by the way their presence is identified.

2. Explosives Vapour Detectors:

These work by bringing the device near to a suspect package. They draw in samples of air and 'analyse' these for the presence of the vapours given off by high explosives.

They cannot detect low explosive chemical mixtures because, in most cases, these give off no vapours. High explosives are hydrocarbon compounds which give off vapours in various amounts. Commercial explosives give off copious vapours while some military explosives give off very little.

Cheaper vapour detectors can only detect commercial explosives, while the more expensive versions can detect many, but not all kinds of military high explosives. The price of even the cheaper versions is way beyond the pocket of the average person. The more sophisticated versions are exceedingly expensive.

The major drawback with vapour detectors is that they cannot detect low explosives, and high explosives can be sealed inside airtight containers from which no vapours can leak.

3. X-ray Scanners:

These are the most expensive bomb detectors, but in many ways the best. Being able to see directly inside a package is very reassuring.

An X-ray scanner is usually a sort of cabinet into which the suspect package is placed. X-rays are passed through the object and an image is created on a mirror. The investigator views this through a window (the screen).

The major drawback with an X-ray scanner is that only metal objects show up properly on the screen. Bombs without metal parts or wires could pass through undetected. This is because an X-ray image is really a shadow. The object in the path of the X-rays absorbs some of the X-rays as they pass through. Paper and even thick cardboard hardly absorb any X-rays at all and therefore cast no shadow. Metal on the other hand absorbs practically all X-rays and therefore casts a heavy shadow. Another danger is that it is possible to create a bomb which is set off by the presence of X-rays.

This is one reason why it should be kept a tightly guarded secret which detecting methods you use, as the enemy could use this information against you.

WHAT TO LOOK FOR

In the section on DOs and DON'Ts it was stressed that package bombs should never be stereotyped. There are no general characteristics by which they can be identified and size is no give-away. A very small letter bomb can be constructed and, remember, only a few grams of high explosive are needed to injure you.

Despite all this, there are often signs which might indicate that a package is a bomb. Ask yourself the following questions each time you receive a letter, package or delivery of any kind:

1. How did this letter/package/delivery get to me? Was it a normal delivery, was it expected, did it arrive out of the blue?

2. Where did this letter or package come from? Do I normally get letters/packages from this address? Check the postmark and sender's address (if any).

3. How long has it taken to reach me from the time it was posted? Has it taken too long to get to me? Check the date stamp.

4. Does the package look as if it has been opened? If it is an item you receive regularly, is it packaged in exactly the way you always receive it or is something different?

5. Does it have stains on the outside? Many explosives are oily and if not properly packaged can leak through an envelope or wrapper.

6. Does it have a strange smell? Many explosives have a distinctive aroma - often of marzipan or almonds.

7. How would the bomb-maker have armed the bomb if one were inside? Look for holes, flaps stuck down, disguised openings, pieces of wire, string, etc.

8. Is it too heavy for what it is supposed to be?

9. Does it feel unbalanced or lopsided?

10. Does anything rattle, move or shake inside? Are there objects inside which should not be there? Tap, shake and gently feel every delivery.

11. Is the letter/package very securely sealed? Too much tape or unnecessary string? Study the envelope/wrapping.

12. Are there any wires, bits of string or anything else observable through the flap or wrapping? Lift flaps and wrappers carefully to see if they are hiding anything.

13. How am I meant to open this? Open packages in unconventional ways, not how you are supposed to. But be careful: look first so that you don't accidentally set off a triggering mechanism by damaging it.