10. THE BATTLEFIELD

EXPLOSIONS

RULES FOR GOVERNING EXPLOSIONS

Home made Bombs for destructive purposes should be at least 5 kilos in mass of explosive (half this amount for high explosives), the first important principle to take into consideration is the creation of the device. An *Explosives* roll should be done by the Games Master in secret on behalf of the player. This figure derives our first multiplier. Secondly, the size of the device is a factor in its destructive power (as is the inclusion of fragmentary elements like nails, ball bearings etc); the effect is graded as per increments of 5 kilos of standard TNT (dynamite of 50% nitroglycerine content). High explosives like RXD or C4 reduce the weight needed by 50% (and ANFO needing 100% more because of its relative low destructive potential).

Thus, if we create a standard explosive device out of 5 kilos of dynamite, the Games Master rolls on behalf of the bombmaker (getting 3 successes) and finally adding a standard damage multiplier of x10

We get 3 x 1 x 10 = 30 points of vitality damage per person within five meters of the blast

Explosive	Multiplier	Primary Effect	Secondary Effect (½ damage)	Fragmentation (¼ damage)
05 kilos	x1	05 meters	10 meters	50 meters
10 kilos	x2	10 meters	20 meters	75 meters
15 kilos	x3	20 meters	35 meters	100 meters
20 kilos	x4	30 meters	50 meters	125 meters
25 kilos	x5	40 meters	65 meters	150 meters
30 kilos	x6	50 meters	75 meters	175 meters

The bigger the bomb created out of standard explosives doesn't necessary correlate into a larger explosion, there is a point where adding more explosive material is counter-productive (if you want more destruction, creating two medium sized bombs might be better, or creating bombs that fragment into bomblets). The fact is the range of effect relatively reduces around the 30 kilo mark.

The Primary and Secondary effects represent the damage inflicted upon individuals within the blast radius of the bomb, the fragmentation represents flying debris within the bomb (or loosened from the various structures around), The multiplier also represents the wounds sustained by the individuals (armor checks can be made to reduce critical wounds, but the actual blast still causes maximum vitality damage).

As you can see, bombs can be horribly deadly, if during the creation of a homemade bomb the roll is *botched*, it will go off (depending upon how badly the operation is botched the individual will suffer damage comparable to *–1* successes triggers fragmentation up to *–3* triggering the Primary effect – with minus successes converted to pluses for working out the relative damage).

The Games Master should consider the amount of cover individuals have within such blast zones, before apportioning damage – using their common sense.

MISSILES

The use of missiles requires the use of the Firearms Military skill; most advanced rockets (like Stinger missiles, Milan missiles and Cruise missiles) have computer guidance, which makes it relatively easier to hit one's target. Whereas RPGs and LAW rockets require a degree of skill to hit one's target on the part of the user. Both however, (for game purposes anyway) are effected by the user's aiming abilities, to target the vital areas of the target.

Introducing Private Bush, our expert on the battlefield…

Private Bush fires a shoulder-holstered Milan missile achieving *4* successes on her Firearms Military roll, we times this by the standard Milan missile multiplier of *x20* doing a total of 80 points of damage to the targeted vehicle. Because of the high explosive nature of the missile, it invalidates the Level 2 Hard Protection rating of the ATV (it would normally be impossible to destroy the armor plated vehicle with standard handgun rounds). The two soldiers in the vehicle have a relative amount of cover, but they will take a percentage of the damage as rolled by the Games Master (one 10-sided dice is rolled to achieve increments of 10%) - 40% is rolled meaning .4 x 80 = 32 points of vitality loss to both occupants.

The Games Master will decide if the vehicle is still usable for transport purposes, taking into account the conditions of the damage (where it was targeted, the total amount of damage and the type of missile fired etc).

FIXED GROUND SITES & VEHICLE PROTECTION

The Assault Terrain Vehicle in the above example has sustained a total of 80 points of damage (to the front of the vehicle), if we look at the vehicles statistics we find the following details *Hard Cover 2 Protection Armor Rating 60 (F40 B10 S10).* This means the vehicle could have sustained 60 points of damage before it was a burnt out wreck. Closer examination reveals more figures relating to the (*F*) Front, (*B*) Back and (*S*) Sides of the vehicle that pertain to the relative levels of armor – obviously most protection is afforded to the front of these particular vehicles. It would have been possible for the vehicle to take a direct hit from a LAW rocket doing less than 40 points of damage (because these rockets invalidate Level 2 Hard Protection as well).

You will find some particular types of flying/diving vehicles specify ratings like (*U*) Undercarriage and the (*T*) Top of the vehicle protection ratings.

Special note: the Milan rocket still would have caused personal damage to the interior troops even if the total damage didn't exceed the 40 points of damage (it could take from a frontal assault. The plasma generated by such HEAT technology can slice through this level of armored protection like butter.

PROJECTILE HARD COVER TABLE

	PROTECTION OFFERED	TYPES
Level 1	Absorb smoothbore sub-sonic gunfire (pistols and SMGs)	Basic Kevlar Vests
Level 2	Absorb other forms of smoothbore bullets (aka hollow-point, explosive, cookie-cutter)	Assault Suits + Basic Lightly Protected Vehicles
Level 3	Offers basic protection from normal rockets, rifles and grenades	Medium Armored Vehicles like ATVs and troop carriers
Level 4	Offers protection of explosive grenades and all types of small arms fire – usually a fully enclosed vehicle housing + basic protection against APFSDS missiles (1/2 damage)	Basic Tank Heavy Armor with reactive armor and Heavy Bunkers
Level 5	Offers basic protection from HEAT missiles (1/2 damage)	Chobman Armored Heavy Tanks

APFSDS stands for Armor-Piercing Fin Stabilized Discarding Sabot, a type of missile which is encased in a two or three-pieced sabot. The sabot is used to encase the smaller warhead, which can be used in higher caliber (therefore more effective) cannons. With the relative lighter weight once the sabot detaches, means the warhead can achieve greater acceleration than most similar weapons, and greater armor breaching capabilities

Chobham armor is a relatively new type of armor explicitly designed to help combat HEAT missile technology. HEAT missiles use depleted uranium to create plasma when the missile hits its target – such missiles don't implicitly require high speeds. Once the missile hits the target an explosion occurs, detonating a shaped charge of depleted uranium which turns to plasma, and is projected into metal armor. This proves highly effective on basic tank armor. Chobman armor manufactured by the British uses interlaced layers of conventional steel armor, aluminum, plastic, ceramic blocks, epoxy and depleted uranium to counteract the capacity of the plasma. However, it still takes relative amounts of damage.

Another form of protection is reactive armor, this armor is relatively simple in design – it basically entails fastening a number of explosive blocks on the outside of tanks, the theory being it propels the explosive away from the tank.

MILITARY HIERACHY

Armies are constructed of a basic hierarchy of units…

Squad: A unit, which generally consists of 6 to 12 soldiers, usually led by a sergeant. This is generally the smallest unit on a battlefield

Section: A section is a medium sized unit generally consisting of 15 to 30 soldiers, such units are generally led by a senior sergeant – the British army uses the term section for a squad

Platoon: A platoon generally comprises of 3 to 4 squads (40-50 soldiers), with a platoon leader (likely to be a lieutenant) and an assistant platoon leader (senior sergeant)

Company: A company consists of 3 to 5 platoons, a headquarters is generally established to service its needs, which is generally commanded by a captain

Troop: A troop is a company-sized unit of cavalry. The British use this term to denote a platoon-sized armored or mechanized cavalry unit.

Battery: A battery is a group of artillery pieces of some kind, generally there will be a company-sized level of personnel support as well

Battalion: Is comprised of 3 to 5 companies, plus a headquarters company. It will generally be commanded by a lieutenant colonel

Squadron: In the US Army a squadron is a battalion-sized unit of cavalry. The British Army it is a company-sized unit of tanks or armored cars

Regiment: A regiment consists of a number of battalions (generally 3 to 5), plus a headquarters unit. A regiment is generally commanded by a Colonel. In the British and French armies, a regiment means a battalion

Brigade: A brigade consists of a number of battalions (usually 3 to 6). It will generally be commanded by a Colonel or a brigadier general (1 star)

Division: A division consists of a number of brigades or regiments (usually three), plus a number of smaller supporting units (battalions or companies). It will generally be commanded by a major general (2 stars); this is generally the largest unit for which such formal table of organization exists

Corps: A corps contains several divisions, the precise number will vary according to the intended mission, plus additional support units. A corps will generally be commanded by a lieutenant general (3 stars)

Army: An army consists of several corps, plus supporting units. It will usually be commanded by a general (4 stars)

FIELDCRAFT

Soldiers rely upon fieldcraft skills to survive in combat zones. One of the most common is camouflage. It requires being wary of every movement you make, you might look impressive walking along with the best flora display on your head, but it can all be undone by an unwieldy footfall.

After a couple of days in the open, one's sense of smell gradually improves and it can end up being an additional vital source of information. It is important to keep clean in combat areas (above and beyond avoiding sores and infections), it may give you away your position and impair *your* sense of smell. Obviously, avoid using scented soaps and aftershaves (they can be detected at considerable distances downwind), and smoking will dull the nasal senses. Poorly maintained fires for cooking will give away one's position – leaving refuse behind at campsites is also a good source of information about the strength, morale and nationality of the former inhabitants. Most professional units will come prepared with plastic resealable bags that all refuse will be carried out of the operational zone in (burying the refuse is to be avoided as animals may dig it up).

DECEPTION

Deception activities are employed in protecting large armies, industrial complexes and airbases; but prove equally effective for small military units. One can dig false trenches, use an empty ammunition box laid upon its side with piled earth around it to simulate the embrasure of a bunker. Fake craters can be made by piling earth in a circle, which may save a working air-strip from being bombed.

On larger scale fake buildings can be constructed out of timber, plywood and corrugated iron. If it is put near a real installation that is now camouflaged – deception being equally about concealing and drawing attention.

Planting fires will attract the attention of aircraft, by putting dummies in reconstructed vehicles on the battlefield; the enemy's resources may be effectively diverted from real patrols (which may conceal vital platoon movements). Plastic sheeting can simulate roads, burning tyres may add further realism to the *bomb-site*, and vitally obscure some ground details from an aerial perspective.

Deception can be further enhanced by the creation of false radio traffic, to help *sell* the illusion.

CAMOUFLAGE

The use of camouflage in modern warfare can roughly be defined as the use of concealment and disguise to minimize the detection and/or identification of troops, materials, equipment or installations. Camouflage is usually achieved by using elements from the natural environment and/or the creation of artificial materials to match the environment.

THE 7 BASIC PRINCIPLES OF CAMOUFLAGE

- Shape
- Shine
- Shadow
- Silhouette
- Surface
- Spacing
- Movement

The principles therefore seek to hide a tank by adding camouflage netting that will destroy the basic shape and its silhouette, removing the shine of the metal by the application of new generation paints (that also absorb a great deal of surface heat as well). Shadows are removed by placing the vehicle in positions where long shadows aren't cast out over the landscape, the surface of tanks sometimes are disguised by using long brush reed-type material. Tanks are rarely clumped together in encampments in their downtime (being obvious targets for bombing), plus the movement routes of most tank battalions are designed to avoid allowing the enemy opportunities to intercept and destroy.

These principles are also useful in designing military installations that look deceptively like other constructions from aerial or satellite surveillance.

PERSONAL CAMOUFLAGE

The activities or personal camouflage are best performed by soldiers in pairs, one should start by applying camouflage cream to one's face, neck ears and hands. A common mistake is to cover the face, but to leave ears, neck and hands uncovered. There are roughly two different schools of thought in camouflage application, the British believe that some skin should be left unpainted, and the US military believe the face should be completely covered in two-color tone creams.

Camouflage Cont…

The pattern should adhere to the 7 principles as mentioned above. You should be seeking to incorporate lines running down the face, breaking up the vertical and horizontal lines formed by the eyes, nose and mouth. One should also use lighter colors on areas of natural shadow like the underside of the chin, and darken high profile areas like the cheekbones, forehead and nose.

The different hues of camouflage paints are designed to match the basic color scheme of the theatre of war the troops are operating in (such as the *Tiger Stripe* design in Vietnam or the *Chocolate Chip Cookie* Gulf War gear), like white, dark greens and browns in Arctic environments. Camouflage paints generally also offer the soldier sunscreen and insect repellant properties.

The modern combat helmet offers elastic loops to take onboard vegetation. One should remember however, that what looks effective in one area of the combat zone, such flourishes elsewhere are likely to stand out like a sore thumb - to deadly effect. One can also attach loops and green nylon scrim netting to pouches and backpacks; care however must be taken to ensure that the brush material is kept secure, and that the gear doesn't get snagged on fencing and other vegetation on route. Such precautions can sometimes make it more difficult to access vital gear in a hurry, which needs to be guarded against.

Guns are an obvious straight line to avoid, applying some scrim or hessian might seem a good plan, but you may in fact be creating points where the scrim snags on working parts, or your grip is compromised. Some militia paint their guns, although professional armies hand back equipment eventually, so using camouflage adhesive tape seems a more acceptable compromise.

PARACHUTE TECHNIQUES

HAHO (High Altitude High Opening: Is a method of air insertion where the parachute exits the aircraft at height up to 9,100m and opens the parachute immediately. Using a RAM air parachute the operator can glide for several kilometers. This mainly facilitates troops crossing borders without entering hostile airspace. A GPS system can also be carried to help with navigation. At such heights paramilitary units often need to carry oxygen supplies to start their descent

HALO (High Altitude Low Opening): This method of air insertion takes place a heights up to 9,100m and the troops free fall until approximately 750m above the ground. It is used primarily to get troops to their destination quickly, as it is relatively silent and the soldiers don't remain in the air for long (so reducing the chances of being spotted). In free fall mode the parachutist will drop at approximately 192 km to 280 km per hour

4 MAN PATROLS

The usual special operations 4 man patrol consists of a medic, demolitions expert, linguist and navigational expert – although they are all usually highly trained in combat as well; others like the United Kingdom's S.A.S also have experts in marine, mountaineering and counter terrorism. Each member of the squad is formerly designated a 90 degree arc to patrol (usually a man on *point* at the front, two watching the sides, and a *trailer* to cover the rear). The distance held between them is usually dictated by the environment, they shouldn't be close enough to be taken out by a single grenade, but able to communicate effectively.

In a jungle they will be fairly close (where it is hard to spot the enemy), but in a desert terrain they could be as far as a few hundred meters apart. Each soldier is required to maintain effective verbal communications with each other member in case of getting separated – as having individual soldiers getting separated can lead to incidents like the infamous British SAS *Bravo Two Zero* mission (where an 8-man squad got split up in the Gulf War of 1991, resulting in some soldiers perishing in freezing conditions and others being captured).

TACTICAL RIVER CROSSINGS

Crossing rivers in patrols is a vulnerable exercise; one should recce the region to find the best place to cross looking for the shortest route from one side to the other, and for the most hidden place where the opposition forces are least likely to patrol. Everyone should simultaneously move across, as maximum firepower will be needed in such a vulnerable position if compromised. Each individual must be careful not to swallow any water (as infections harbor in open water). Each soldier should cross using their bergens (backpacks) for buoyancy (each pack will hopefully be watertight as when made). Hopefully, they will avoid leaving behind telltale tracks where they have crossed. Four man teams should move across like standard patrols (behind, left, right and point). They should have a spot picked out on the opposite river bank to aim at, on the other side they should exit the river, whilst one remains in the water keeping an active lookout. Efforts should be made to cover their tracks on the riverbank.

TRACKING

HOW TO TRACK

When one is tracking, one is looking for evidence of disturbed grass (track signs – known as *spoors*); the bent blades reveal the direction of travel. The top grass will point in the direction the person is walking. If the person has walked through the area after sunrise the dew will be disturbed and the faint dark area will reveal the trail. Always keep an eye out for broken spider webs or cobwebs; they are useful hints of activity. When looking at Spoors keep your head slightly up and look 15 to 20 meters ahead of you – this will enable you to see the Spoors better and determine the direction of movement. Keep alert for any likely ambush areas.

Look for any overturned rocks, the dark side you will see a matching section of ground. The rock will dry quickly, the ground will show a level of moisture as well – if a rock is still wet, you know your target is probably less than 2 or 3 hours ahead on a sunny day. If you find it at sunrise, you will know he has been moving before sunrise.

The darker and wetter the rock, the closer you are to your quarry.

Tracking Continued…

The art of tracking generally comes down to looking for things out of context in nature and realizing the cause. Always be sure of the last sign, before venturing too far forward. There are obvious signs, like muddy footprints near streams and water holes and sandy rivers, leaves on plants broken (or turned so the light underside contrasts with the surroundings, scuffed tree bark or mud knocked off and the impression of rifle butts or walking sticks. Indeed, blood on vegetation might be present.

Look out for discarded ration packages, food tins, smoke butts. Certain armies and paramilitary groups may wear the same type of boots (patterns in dirt), you may well be unnecessarily tracking one of your own troops!

You might even take pictures for your own records. Local intelligence communities may already actively catalog such activities, so check if records are available. The depth and space of the track may also tell you something about your quarry, women take smaller steps (as do heavily laden men), people running leave greater spaces between steps. People walking in each other's tracks will make deeper impressions, plus the edges of the tracks will become less distinct. Any drag marks could indicate a wounded soldier. If the tracks split keep following one set, sometimes guerrillas will split up or *bombshell* – they will try to throw someone off following by splitting up. Even if this is the case, the odds are the team won't be apart for too long (and the tracks will once again converge). Always remember, you may be ambushed at any stage…

STICK & STONE NAVIGATION

It's all perfectly well if one has a compass, but how do you know the way home after an ambush, or you have escaped from enemy capture without your possessions? The old stick and stone method is taught to special operations experts.

You'll need a stick about a meter long and two pebbles.

Firstly, place the stick in the ground and then place a pebble at the tip of the sticks' shadow, then wait for 20 minutes. After 20 minutes the shadow will have moved away from the stone, once again place the second stone at the tip of the shadow. Then lay the stick across the two stones, this gives you a line pointing East to West. Now place your left foot by the first stone, and your right by the second stone, with the sun on your back, you are now pointing Due North.

Another method is accomplished by using a mechanical wrist-watch. Point the hour hand towards the sun, and use a small twig to cast a shadow down the hour hand through the central pivot – then divide the distance between the hour hand and the twelve o'clock position. This will give you the North – South line (North being always the furthest from the twelve o'clock position.

CLOSE TARGET RECCE (CTR)

The use of close target recce (CTR) is important to gather essential information about target facilities. Without such a detailed knowledge, operations may well be poorly planned and lead to unnecessary risks. Planning is important in successful CTRs; considerations of time, risk, team numbers and designation of emergency rendezvous points can mean the difference between success and failure. The first consideration is whether the team will be heliborne near the target, or walk some distance to the target, parachuted in, or even canoed in. The patrol once at the general area will make their way to the Emergency Rendezvous Point (ERV). This place will hopefully have been selected to provide a great deal of cover (especially in the case of a team having to defend themselves against hostile forces if the mission is blown). The team will have probably been issued with a couple of nights of cold rations (just in case of the evacuation doesn't go to plan, plus they don't need to make fire). Here they will generally leave their bergens (backpacks) and make camouflage arrangements by the picking of suitable flora. In eight man teams, it may be that 2 of the men are left behind to guard the ERV site, whilst the other 6 men go off in pairs to find O.P (observation posts) – of these remaining men two soldiers will find O.Ps behind the target, 2 in front of the target – whilst the 2 other men guard the retreat positions for these observers.

The teams may well swap over at night if it is a long CTR (some CTRs may well be measured in weeks). The O.P positions are manned by two individuals, once established they begin the *Hard Routine*, being they will monitor in turns the enemy using binoculars and recording everything with infra-red cameras. They may well swap over every hour (although 40 minutes is recommended as it gives the sleeper time to restore vitality and vision, but not fall into REM sleep – which makes one drowsy). Special emphasis in observation is given to recording the number of troops, patterns of movement, weaponry, surveillance equipment, lighting, automatic defenses, dogs, buildings entrances/exits and possible entry and exit points.

FIBUA (Fighting In Built Up Areas)

Fighting In Built Up Areas is a vital skill for the modern solider. Most of our modern battles have been fought in such areas as Bosnia, Iraq and areas of Afghanistan. With most Third world's countries slowly changing from rural subsistence economies to industrial, the vast majority of future battles will take place in such restrictive environments. As Operation Iraqi Freedom drags on in the Middle East, it is easy for even the most technologically advanced armies to get bogged down in firefights in the maze-like back streets of Baghdad. The fact is the odds between a weaker force and its stronger foe are reduced substantially.

The common factor between defending and attacking forces is the considerable stress such combat creates, and the need for specialist training for urban environments.

A factor to keep a look out for is the humanitarian one, looting and unnecessary damage to buildings may alienate the force, and the help of the local civilian population should never be taken for granted. Besides, blowing up buildings creates rubble, blocking routes and gives the enemy cover. Lack of authority displayed over looting offenses may create a lack of discipline in soldiers and may lead to weapons being discarded to carry more booty.

DEFENSE

What are the preparations one should take to defend a built-up area?

One should seek to have good fields of fire and command routes that the enemy is likely to use in entering the city. You should also choose a strong building, as many modern buildings are built with thin walls attached to a steel or concrete frame, and may also have large windows. An ideal building is one made of stone, brick, or reinforce concrete. It will hopefully have more than one floor, and a basement. The upper floors will absorb artillery and mortar fire, whilst the basement serves as a good place to treat the injured, store food, water and ammunitions.

Before the firefight begins the building should be prepared for a defense. You should remove all glass (which in an explosion turns into lethal projectiles), putting chicken wire across the window frame will prevent grenades from entering. Net curtains should be left intact (as they provide visual cover from outside observation, but not out), hessian can be substituted and nailed to window frames.

The building should be reinforced with timbers supporting the floors inside. Sandbags should be used to block the front door, thicken walls and floors – this will protect against fragmenting (plus, they are handy to create bunkers inside buildings). Such bunkers provide protection for machine gun crews, if set about 1 ½ meters back from the window – the gunners will have a restricted field of fire, but the payoff is that the flash, smoke and dust of the weapon won't be observed from outside.

Embrasures should be set into the roof or under the eaves, or made by knocking out singular bricks in the walls. Anti-tank weapons are best employed on the roof, as the enemies armored vehicles may be thinly protected on the top. The use of infantry and anti-tank weapons above, also create a vertically and horizontally potent layered defense. Fake embrasures can be painted in black on the outside of unused buildings to confuse the enemy.

Window sills should be blocked up by boards peppered with studded nails, stairs can be sawn down or strung across with barbed wire and doors can be studded with nails. Movement within the house should be achieved by ropes or ladders through a hole through to upper floors (to make it hard for the place to be stormed). Barbed wire can be liberally strewn through existing natural obstacles like hedges, fences and walls; and can be used to block access to roofs. Drainpipes and thick creepers should be removed from buildings to stop climbing opportunities for the opposition. Exposed live wires can be hacked and scattered as a shocking deterrent.

Before the actual battle takes place water should be collected in all available containers (including sinks and baths), as you may be ensconced for a while, and it is also handy to have about for putting out spot fires.

Mines both anti-tank and anti-personnel (plus booby traps) can be used to funnel opposition forces into selected *killing grounds*, as well as slow down the opposition.

Although forces should try not to concede ground, exits should be pre-planned for escape into adjoining buildings (through walls) or into sewers if the opposition is overwhelming.

The main characteristic of such measures is that the defender's most effective tactics are to engage the enemy – passive tactics are counter-productive, as it gives the enemy time to make alternative plans that may undo preplanning. Fighting patrols, screens of infantry and armor that can withdraw whilst causing casualties into preplanned defenses and obstacles work the best. By causing such erratic displays of attack and retreat, the enemy doesn't have time to take the initiative – theoretically you could lead the enemy on a wild goose chase all around town. If the enemy can't work out your forces and tactics, they may never breach your main defensive stronghold.

Air power is only ever of use before opposition forces enter the city, it is rare (even in these laser targeted missile days) that a commander will use air power to support troops engaged in close combat in built-up areas. So apart from combat helicopters like the U.S AH-64D Longbow Apache, it is rare for air platforms to enter into urban combat zones.

ATTACK

The major aim of any attacking force will be the ability to take the city in bite-sized chunks. Basically, attacking the town block by block, building by building, securing it and moving on to the next one. Obviously, it rarely happens in such an ordered way. A smart enemy will want the invading force to be tempted into their ambush and retreat cycle – it is imperative that in responding to the threat the attackers do not get caught up in following up such attacks and be drawn deeper amongst unsecured buildings.

The use of anti-tank weapons, the main armaments of Infantry Fighting Vehicles (IFVs) or Main Battle Tanks (MBTs) can be used to blast positions. This can kill or stun defenders, but also creates access points for troops through the blasted walls.

Specialized equipment like Bangalore Torpedoes help clear away barbed wire, satchel charges can blast strong points. Flamethrowers obviously kill by burning, but can also have the added effect of consuming oxygen in cellar regions and starting spot fires. Bursts of flame can effectively be *bounced* around corners, one can even alternate by using wet shots (gasoline fuel) and a dry ones of burning fuel. It may even be enough for the defenders to surrender, knowing they are covered head to toe in fuel.

One should also look out for defenders using flame weapons in the form of molotov cocktails.

Smoke and CS grenade canisters can be used to flush men out of cellars and sewers, while white phosphorous grenades can be used to create smoke, or even as an anti-personnel weapon.

The commander should ideally seek to clear the buildings top downwards. Most soldiers have been trained in the skills necessary to utilize ladders, grapnels and ropes, as well as training to enter into windows or rolling out of sight on the top of roofs. Most special forces troops practice heliborne operations, like abseiling and fast-roping. Once the troops are on the roof, it is a relatively simple task to roll grenades down the stairs, bursting into the rooms with rifles at the ready, and flushing out the resistance. Procedure dictates that the soldier will back against the wall and shout ‘Room Clear!’ before moving on.

The attackers should seek to avoid standing in open streets or public spaces, which will invariably be factored into the defense plans as the *killing grounds*.

All combatants should seek to backup into the shadows away from windows, look around corners at ground level and avoid creating a silhouette or shadow where walls and windows make straight lines.

One way to move through a built-up area is through back gardens and sewers, or blasting holes in adjoining buildings (otherwise known euphemistically as *mouseholing*). Some basic idea of building design can help in locating weakened walls.

Attackers do not want to be drawn into traps, or to get ahead of casualty evacuation areas or ammunition re-supply points, but at the same time they do not want to give the enemy time to regroup, or counter-attack. It can be a difficult balance to achieve.

For both sides, fighting in built-up areas uses up very high rates of ammunition. Ranges can be very short (like room-to-room) so casualties can be very high.

Sewers, underground railways and service tunnels can be used effectively to move men and supplies forward undercover, but the enemy may well have booby-trapped these resources.

BUILDING CLEARING

Movement in close quarters is of critical importance, it is always much easier to accomplish in two-man or four-man teams. It is of importance to know all avenues of egress, as many buildings conceal obstacles, hostile forces and traps ready made to give away one's position.

1. Hallways are an easy feature to negotiate in enclosed spaces, trouble invariably being in front of one, than behind (the area previously explored). T-junctions however are a little different, it is generally S.O.P to slowly look from one side (getting a look partially up the junction, but not looking so far as to expose your head to forces up *your* side of the junction), whilst your companion waits at the other side. Then it is repeated on the other side of the junction – it doesn't give one complete knowledge of long t-junctions, but it involves a great deal less risk.
2. Open Rooms – Large rooms, especially in low light, provide ample positions to be surprised by hostile forces, the best practice is to keep complete coverage of one side of the room (by moving along the wall with a weapon pointed towards the center of the room, scanning whilst moving). It is important to not send an additional force down the other wall simultaneously, as friendly teams under attack may shoot each other through opposing arcs or fire.
3. Doors – Doors can be open, closed, locked or unlocked. If the door is open the use of the cross maneuver is preferred. This can be performed by 2 or 4 man teams. In the two-man variant soldier 1 moves to the left hand side of the door, whilst soldier 2 moves to the right – soldier 2 then opens the door, and soldier 1 either throws a flashbang grenade or moves into the room on the right side. Soldier 1 will lay down cover at a 45% angle from the front of the room to diagonal on the right hand side, soldier 2 will now move in the left hand side of the room and lay down cover from straight ahead around to the left. In the 4 man variation, the two other soldiers move in behind the two lead soldiers (just in side the door on either side) and scan the back wall for foe. There is also a variant used in covert entry which has both lead soldiers looking into the room before entering (soldier 1 on his knee looking left, soldier 2 standing looking right). If the door is closed but not locked, soldier 2 opens the door on soldier 1's count. If the door is locked it can generally be opened by a pry wedge (crowbar), ram, lockpicks or shot out with a charge or a hatton round from a 10 gauge shotgun.
4. Twin Doors – When two doors open in a hallway directly across from one another a four man team is desirable, the theory roughly works similar to a two-man breach of a singular door, the object is to make sure you aren't surprised by enemy from behind by all going through the one doorway. If there are multiple entries heading the same way, it is important not to split the team up. It may be necessary to open one door and enter through another, it might buy you some valuable time (and reduce the risk of friendly fire).
5. Stairs – Are difficult tactically (there is always an invisible portion for enemy to hide both up and down). If stealth isn't important covering fire can be laid down. However, one soldier moving ahead whilst the other watches for threat above should gradually mean the team can work its way up or down stairwells with relatively safety.

SURVIVAL

A standard survival pack of any soldier should include the following…

- 10 wooden matches
- candle
- magnifying glass
- needle and thread
- fish hooks and nylon string
- compass
- snare wire (20ft)
- flexible saw
- 2 surgical blades
- 4 condoms (can hold up to 1/2 liter of water each)
- 12 bandages
- water proof pouch (large enough to hold all items)
- mess tin (aluminum with clip on lid)
- survival bag (heat insulated bag of reflective material to keep warm and dew free)
- a coil of rope (15m)
- roll of kite string (80m)
- flashlight and batteries
- 2 large garbage bags
- 3x4 m tarp

EDIBILITY TEST

The following procedure should be performed upon any food source you are unfamiliar with, or are unsure that it is ready to eat…

1. Inspect: Try to Identify, ensuring the plant isn't slimy, worm-eaten or old
2. Smell: Crush a small portion (if it smells of peaches or bitter almonds - discard)
3. Skin Irritation: Squeeze some juice or rub slightly on to tender skin (like the underside of upper arm). If discomfort, rash or swelling occurs – discard
4. Lips, Mouth, Tongue: If there is no irritation thus far follow the following steps in 30 second intervals, whilst checking for irritation or a reaction

- Place a small portion on the lips
- Place a small portion on the corner of the mouth
- Place a small portion on the tip of the tongue
- Place a small portion under the tongue
- Chew a small portion (do not swallow it yet)

Swallowing: Ingest a small portion and wait for 5 hours (don't eat or drink anything else during this period

Eating: If no reaction occurs (eg soreness of mouth, repeated belching, nausea, stomach or abdominal pain) – the plant can be considered safe

Collection of Food from the Wilderness
There are potentially many food sources in the wilderness, but precautions (in addition to the edibility test above) should be observed…

1. Gather Plants Systematically: Take a container along on foraging trips to avoid crushing plants that may go bad
2. Leaves and Stems: These may be edible, and young growth will be more tender and tastier
3. Plants Roots and Tubers: These are often edible, choose larger plants for a bigger supply of food
4. Fruits & Nuts: Many plants with ripened fruit are good sources of nutrition. You can tell if a fruit is ripe if it is firm when squeezed gently. Hard, green berries are indigestible. Peel fruits with tough bitter skins. Nuts are ripe when they fall from the trees, shake trees with stick or strike branches and see what falls. CAUTION: Some seeds and grains contain deadly poisons. Perform edibility test and discard anything that is bitter and hot (unless identified as pepper or spice). The heads of some grain plants have enlarged black bean-like structures (instead of normal seeds) – these carry poison, hallucinogenic, or fungal diseases that can be lethal.

Edibility Test Continued…

5. Fungi: Can be plentiful in wilderness, but you must be careful. Pick medium to large sized specimens for identification. Store separately, as some poisonous fungi can contaminate other food sources. There is no edibility test for fungi, deadly kinds do not taste unpleasant, and it may take several hours after eating for symptoms to show. There is also no truth the folk tale that fungus is not poisonous once peeled, or that poisonous varieties change color when cooked. The only way to tell the difference of poisonous varieties is that poisonous ones have…

- White Gills: Fine feather like slits on the underside of the cap
- Cup Like Appendage: At the base of the stem called a volva
- Rings Around the Stem

6. There are two common poisons that are naturally present in some plants…
- Hydrocyanic Acid (Prussic Acid) which tastes and smells like bitter almonds or peaches
- Oxalix Acid which is recognizable by a sharp, dry, stinging or burning sensation when applied to tongue or skin

7. Some General Rules about Plants to avoid
- Plants with milky white sap (unless identified like dandelion)
- Plants that are red
- Fruits that are divided into 5 segments
- Plants with tiny barbs on stems and leaves (will irritate mouth and digestive system)
- Old or wilted leaves, as some species develop deadly toxins when wilted

SHELTER

HOW TO CHOOSE A GOOD CAMPSITE

Local conditions and materials available should determine where to set up a shelter; whilst there is still daylight, scour the vicinity to look for the best natural shelter from wind, rain, and cold before nightfall (you may not prepare your own shelter in time).

Your main concerns are providing shelter that avoids wind, rain and flood

BAD PLACES TO SET-UP CAMP

- Exposed Hilltops (seek shelter on the leeside)
- Valley Bottoms and Deep Hollows (these are damp, flood sites and liable to frost)
- Hillside Terraces where the ground holds moisture
- Spurs which lead down to water (usually animal routes)
- Too Close To Water, where insects and heavy rainfall may cause the river to swell
- Near solitary trees, which may attract lightening
- Near Bees or Hornets nests

WHERE TO CAMP

You should choose a place that is sheltered from wind, near water and possibly somewhere with access to wood. If you are in forested areas, check above for dead wood in trees (that may crash on you during the night). The sound of running water nearby may drown out other noises. Do not camp across a game trail.

TYPES OF SHELTER

TEMPORARY SHELTERS

Bough Shelter: A branch that is partly broken and is resting on the ground may provide the basis for a temporary shelter, one can even remove the broken branch and place it in the fork of another tree for better stability. A variation in snow is digging into the snow under a fir-tree and picking some fronds to make a space between your body and the ground (which also allows for circulation of air to dry your clothes)

Root Shelter: By spreading around roots and earth at the base of a fallen tree, you might create an effective windbreak, you can even fill in the roots structure of a large tree and nestle inside

Natural Hollows: Any shallow depression will provide protection from wind, although if it is on a slope, some kind of effort must be to deflect water filling the hollow

Stone Barriers: You can build up a wall of stone, earth and roots to provide a windbreak

Parachute Tent: If one is dropped behind enemy lines with minimal resources available an old fashion bell parachute secured in an overhanging branch and pegged around the outside with sticks creates a functional shelter

Additional: if your shelter is below ground level, create a trench around it to redirect water

LIGHT STRUCTURE SHELTERS

Sapling Shelter: By gathering suitable saplings you can create a v-shaped structure (tied to a central sapling pole with vines, the other ends are forced into the ground. Over the top a tarpaulin can be placed (or the saplings can be placed closer together and filled in with vines and roots).

Shelter Sheet Tents: This construction requires a waterproof poncho, groundsheet, plastic sheeting or canvas. Using a central piece of wood, a triangular shelter can be constructed (the point facing into prevailing winds, held down with rocks. The floor should be covered with dry grass or bracken for bedding – to keep one off the cold earth).

Teepees: The quickest type to erect using three or more central poles, leave an opening at the top for ventilation. Make sure to secure the teepee to the ground.

Snow Cave: A shelter cut into a depth of snow of around 2 meters or more (the inside roof is domed). Once the inside is dug out (usually taking a soldier an hour), a well is dug near the entrance (to draw down the cold air). Once inside the cave, a candle should raise the temperature to a comfortable level.

Pole Bed: Creating to A-frames out of poles and tie with string or bark, and prop it against a tree (with additional poles to create a bench), you can create a good platform to avoid sleeping on cold earth. A mosquito net over the top however, may mean the difference between *sleeping* and dozing in a jungle environment

HOW TO BUILD FIRES

Fires are essential to survival, providing warmth, protection and a means of signaling (it evens boils water, cooks, and preserves food) – so it should be a priority.

Firstly, heat dissipates in the wild quite readily. If you want greater warmth in your shelter, placing rocks around the areas will reflect it back into the space.

To Light a fire remember AIR, HEAT and FUEL.

Preparation: Ensure there is adequate ventilation for the fire. The more oxygen introduced, the brighter the fire will burn. Alternately, by reducing ventilation the fire will burn less, but need less fuel.

Building Fires Continued…

The Fireplace: Choose a shelter site, do not light a fire at the base of a tree. Clear away leaves, twigs, moss and dry grass from a 2 meter area until you have bare earth. If the ground is wet or snow covered, build a platform of green logs covered by a layer of earth or stones. If it is windy, dig a trench to light the fire in, or circle the fire with rocks. The rocks can serve as heated pot stands and bed warmers.

Tinder: Choose material that takes only a spark to ignite. Birch bark, dried grasses, wood shavings, bird down, waxed paper, cotton bluff, fire cones, pine needles, and the inside of bird nests make great tinder

Kindling: This is the wood used to raise flames from tinder, small dry twigs and softer woods are best. You can make fire sticks, which are sticks with small cuts up and down to feather them (that will catch more readily).

Fuel: Use dry wood to get the fire started, once it's established mix green and dried-out damp wood

Hard Woods, such as hickory, beech or oak burn well, and are long lasting
Soft Woods, burn fast and give off sparks, the worst being alder, spruce, pine, chestnut and willow
Green wood does not burn particularly well. Lay them tapering away from wind, so they shelter the fire, whilst they dry

Save energy, there is no need to chop up logs, break them over other logs, or just let them burn over the fire – but always watch the fire

FIRELIGHTING

To light a fire you should do the following

1.Create a teepee of kindling around a tinder bed
2. If it is windy, lean kindling against a log at the leeside
3. Ignite tinder using one of the following methods

Using a match, carry the non-safety type in a waterproof container, and split them in half to make them last longer – remember not to use more when a fire source is established

Sunlight through a lens, you can use a magnifying glass (or any other type of lens) to focus the sun's rays to form a white hot spot pointed at the kindling, keep out of the wind, and blow gently until a small flame ignites

Flint can be struck against steel or another hard surface close to the tinder, that a spark will fall on; blow gently once the tinder is smoldering

4. Add larger sticks or tinder bundle until the fire is established.

Yukon Stove: This particular stove constructed around a fire is made from stones, rocks and mud. Basically, the individual makes a round base, much like a tortoise shell at the top – remembering to allow a hole on one-side for fuel and air. It is also desirable to inset an old tin can or metal box, but not necessary. The top of the stove can quickly cook oatmeal cake type portions, eggs, dry leaves for tea, meat etc. One can even recover the charcoal from underneath to help re-odorize boiled water

Did You Know: British SAS soldiers in Borneo in the early 1960s spent up to 6 months in jungle environments on long range reconnaissance missions, sometimes without radio support. By the time they emerged from the jungles, their clothes were literally decomposing off their backs.

TECHOWAR

THE HIGH-TECH BATTLEFIELD

The strive for advantage on the battlefield has always driven innovation, from Leonardo DaVinci creating war machines for Florentine Patrician's in the 15th century, through to modern American Aerospace industries trying to create working missile defense systems. The modern battlefield has a number of devices like sensors to detect enemy activity, computerize fire control systems, through to communications systems sending out orders via frequency hopping, short-burst (and encrypted) radios. There is also the use of GPS systems to keep track of troop movements, thermal imaging, passive IR technology and image intensification.

The basic principle in communications is to preserve the force's C3 (command, communications and control systems) from interception, decrypting and jamming – whilst providing countermeasures to prevent the opposition from doing the same. Despite the relative technological advantages of high-tech defense forces, it is still possible for them to be compromised by the use of readily available high-street scanners, jammers and radios.

Often the ingenuity of one radio operator/decrypter is enough to change the fortunes of war.

Missiles can be launched at a safe distance hundreds of kilometers away from the target by GPS-guided systems, which may use satellite technology to identify a viable target – a soldier may never need to set foot upon foreign land to dispose of known existing command centers. Some military soldiers have access to helmets mounted with video cameras, which relay real-time images back to the commander. Other technologies include IFF technology (Identify Friend or Foe) which gives a visual display inset in one's goggles to show viable targets digitally overlayed with relative ranges. Another complimentary technology is the HUD (Heads Up Display) unit, which allows for a soldier's gun to be linked to the goggles display to show where they are aiming. Such units can be used to order target priorities according to the commander's whims. Add to this the power of thermal imaging, image intensification, and the battlefield is a very different environment.

Satellite Communications SATCOM: This system currently forms part of the British Special Forces operational setup. The communications are facilitated via static, mobile and portable units, the later weighing around 10kgs. They operate on UHF and SHF frequency bands. British forces use Skynet 4 and 5 series satellites for operation purposes (which are in geosynchronous orbit). Such a system provides constant communications links worldwide. Once the transmitter/receiver is setup it will track the nearest satellite. Signals are transmitted on one frequency, and retransmitted in a different frequency by the satellite (whilst boosting the signal).

DIGITAL COMMUNICATIONS

The U.S army has invested heavily in developing systems of control and command that deliver more information and flexibility to orchestrate operations quickly and effectively. Part of this process is the Force 21 Battle Command Brigade and Below System. This is effectively an intranet based satellite encrypted system that links up a network of computers, radios, routers and integrated equipment for all aspects of operations (command and control, platforms, troops, UAVs, laser designators, satellites et al). The information is processed to provide location exchanges, status information, transfers of specific communications between specified members and command orders. This is generally facilitated by a team of soldiers in portable computer centers deployed at short notice to somewhere near the combat area. It is designed to give the higher echelons the ability to access more information, and to restrict each platoon to receive only pertinent information (as too much information can be as debilitating as too little).

The system includes a GPS system that facilitates the supply of information to all friendly forces in the immediate area; the system also has the capability to track hostile forces once identified. The computer interface shows a digital map updated in near real-time, the wireless system network also shows basic terrain mapping. The system seeks to keep the vehicle centered upon the screen, and allows for flexibility in scanning around the battlefield to coordinate movements.

The system is touted as being a 'tactical internet', whereby soldiers can enter an on the *spot report* on any location, which can be relayed to brigade-level intelligence officials. The enemy is then recorded on screen as a red symbol (denoting enemy). An UAV can further be deployed to gather more information on the enemy unit.

The system even designates different friendly *platforms* (the military name for vehicles) with different blue symbols; the system even represents battalions with larger blue rectangular icons. The system is designed to be fitted into the left fender of vehicles (the EPLRS – Enhanced Position Location Reporting System), a computer screen and keyboard is installed somewhere inside the vehicle. A hook dialogue box is indicated upon the screen that can be opened by the operator to get an on the spot report from nearby vehicles.

The system is designed ultimately to speed up the process of command.

Other similar systems are in development, or are being used in limited capacities by other forces.

NIGHT VISION

The development of passive light systems in recent years may overlook some crucial basic countermeasures that can still prove effective. Human eyesight is still useful in seeing objects at a distance, especially if combined with binoculars. It is often a lot easier to discern useful information by looking unaided than through thermal imaging. The glint of moving objects, the smell of firewood burning and the use of flares projected over the landscape often relay more information, than just seeing your standard IR heat blobs on the horizon.

Basic Active IR entered service during the Second World War, often vehicle lights were taped over by IR jelly-like film, and the road was viewed through special IR filter binoculars – however, anyone else having similar binoculars could see the vehicle lit up like a Xmas tree. Active IR is likely to still see service today in some poorer countries (rarely does old military equipment get melted down, just sold on).

IMAGE INTENSIFICATION

This passive system amplifies the ambient light from man made or natural sources (like the moon and the stars). It entered service in the 1962-75 Vietnam War (nicknamed the Starlight Scope). Basic modifications to lens technology adds a degree of light intensification, it also had the attraction that a new lens could be fitted to most standard cameras. A basic British Army Common Weapons Sight (CWS) - the Pilkington Observation Sight adds an additional 4x to 6x magnification level, and one can recognize a man standing at a range of 450 meters in starlight conditions. This 3rd generation sight is aided by hardware which reduces the *blooming effect* (the blinding effect of looking at intense light sources like car headlights); the sight improves the light intensification capabilities by around 20,000 times. Such technologies can now be purchased in goggle forms for relatively cheap prices.

Image Intensifiers do not function particularly well on overcast nights in remote locations, and prove virtually useless under thick cloud cover.

THERMAL IMAGING

The basic advantage of thermal systems is that heat sources can be viewed even if they happen to be standing behind light scrub, vegetation or smoke. It has been used extensively in search and rescue missions since its first use by the British Army in the Falklands War in 1982. Problems arise in its use by untrained soldiers, as the heat signals aren't always immediately classifiable – as operators in the Falklands war often mistook the heat signatures of sheep to be crouching soldiers. Modern systems are no more bulky than a video camcorder.

Thermal imaging works by scanning the visible band 0.4 to 0.7 microns and 0.7 to 12 microns in the infrared spectrum. It can even pick up the heat sources from fresh tank tracks in mud and water warmed by engines dispersed from the wake of a ship.

Problems arise with such systems at long ranges, the heat signatures can become confused, as most heat sources turn into indistinct heat blobs. This has led to some unfortunate *blue-on-blue* friendly-fire casualties in the Gulf War (soldiers generally have a blue heat signal, they became mixed up with Iraqi targets at distance).

Thermal equipment doesn't perform well in rain or sandstorms, severely limiting the effective distance.

EVADING THERMO

There a number of techniques used on the modern battlefield to evade thermal imaging…

Smoke screen projectors are now sometimes loaded with grenades like the US M76, which produces a standard smoke screen, but with hot fragments, which descend slowly. Modern tanks are now fitted with laser warning systems that detect when it has been *lazed* by a rangefinder, and automatically fires heated infrared (IR) smoke to cover a hasty withdrawal. T.I camouflage nets are now available, which can completely mask the thermal signature of a man or vehicle – but they are usually designed to filter out *some* heat so that a thermal *black hole* isn't produced. Problems can arise with such countermeasures, as thermal screening can literally *cook* soldiers in vehicles or under cover in their own heat.

BASIC TACTICS

A good understanding of *S.O.P* (Standard Operating Practices) can help to evade the use of thermal imaging; like avoiding open spaces by day or night, the use of dead ground and effective cover when you are on the move. A patrol moving evenly spaced, across a field at night leaves little to the imagination of a trained user of thermal imaging. Thicker forms of vegetation can conceal a man, as well as walls or buildings.

The best place to be is in urban environments, but even here caution should be taken to not *act* like soldiers (like forming in queues for food, parading in three lines, or *skulking* of a tactical variety). Obviously, putting vehicles into garages or barns helps to hide their heat signatures.

ON THE RUN

If one is trying to avoid pursing soldiers, or even police in urban areas – one should seek to maximize one's chances by taking into account some shortcomings in the technology. One should blend into the urban clutter of other people or vehicles. Underpasses, tunnels and cuttings give an opportunity to lose pursuers, and even change vehicles. If one suspects they are under TI surveillance, they should seek to act naturally, and make use of the prior tips. If one is hiding out, you should remember such technologies don't perform well in falling rain, snow or sandstorms (even aircraft may well be grounded in such weather) – plus, snow and sand covers tracks and muffles noise. Besides, most guards in such weather are less alert.

Remember, at long ranges the image becomes attenuated - one blob acting naturally is indistinct to the suspect acting naturally.

LASER DESIGNATORS

The stunning use of laser guided missiles in the 1991 Gulf War has actively masked a major problem of these technologies – often the bomb might hit the designated area (85% ratio), but the underlying problems of limited intelligence might mean you have just wasted a $US3 million dollars hitting a foreign embassy (as the United States managed when it targeted the Chinese embassy in Bosnia – needless to say, they weren't pleased).

Recently in Afghanistan, the U.S deployed two man special operations teams with handheld laser designators to target Taliban targets, which proved extremely effective. The units work primarily by projecting a beam of light at a targeted structure, or vehicle – the beam of light hits the target and the positional information is then relayed to command. It is then that a Laser Guided Bomb (LGBs) is designated to the target and dispatched. Such handheld units have 10x telescopic zoom, image intensifiers and thermal imaging accessories; they generally come with a tripod (for stability in focussing at long ranges). The unit can designate targets up to 10 kilometers away. The use of laser designators is seen as the future of warfare where the objective is the outright destruction of the countries potential to wage war (rather than invasion).

SENSORS

Ground sensors are common place in modern warfare; they are generally spread over a wide area, or used to assist in close range contacts (like in ambushes). Since the 1970s the United States has refined its remote sensors system the Martin Marietta REMBASS (the Remotely Monitored Battlefield Sensor System), plus the improved version (IREMBASS). The British have developed a variant known as CLASSIC (Covert Local Area Sensor System for Intruder Classification). CLASSIC uses TA2781 Sensor Units, which with its radio transmitter has a range of some 21 kilometers (and a battery life of 90 days). The unit is either linked to a MA2743 seismic, MA2744 passive IR, MA2770 magnetic or MA2772 piezoelectric cable sensors. When the sensors detect movement the TA2781 transmits to the RA2786 monitor unit that produces an audio or visual display. The output can be printed out for a hardcopy of troop movements, the secured information is transferred to HQ and the MA2775 data interface can show movements on a computer-generated map.

The seismic system measures vibrations through the ground, it has a range of 1 to 150 meters (depending upon ground conditions) and can identify personnel on foot, tracked or wheeled vehicles. The passive IR beam on the MA2744 has a two directional path – that indicates the direction a man or vehicle is moving. It has a range of 60 meters (but up to 300 meters for some heavy vehicles.

The MA2770 magnetic unit will pick up the mass of a vehicle, or if two units are present, can indicate their respective directions. At 5 to 20 meters it can detect cars, 10 to 40 meters tracked vehicles - it can even tell if a soldier is carrying a rifle at 1 to 10 meters.

The MA2772 piezoelectric cable is dug into the ground just below the surface, and it can stretch for up to 750 meters. There are two different types of cabling: the high sensitivity cable for detecting personnel, or the lower sensitive one that will indicate vehicle movement – they both will indicate the direction of any movement.

The CLASSIC TA2781 can also use pressure pads, contact switches, trip wires, inertia switches and NBC sensors. A relay unit known as the RTA2785 can be used to increase the range up to 30 kilometers.

CAD COMPUTER AIDED DESIGN

A relatively new development in the area of operational planning and anti-terrorist work, the use of CAD software to input environmental factors of the area of operation into a 3 dimensional virtual space, this greatly enhances the co-ordination of the team. Such systems allow for room details like windows, doors and routes to and from the building to be modeled – a soldier can be virtually led through their particular route of entry (such systems can even include scans of photographs of the interior of the building for added realism).

CYBERWAR

The destruction of the control systems of major public utilities (water, gas, electricity) during wartime is equally as important as the bombing of key military installations in the primary phase of operations. Ultimately, such utilities in the 21st century are controlled by computer systems. Other targets controlled by *bits and bytes* include air traffic control systems, communications networks, military command and control systems, and computerized surveillance infrastructure. With the United States armies increasing reliance upon computer automation of its troop movements (as part of its *transformational doctrine*), it is little wonder then that opportunity beckoned for an 18 year old Israeli youth to hack into the Pentagon's system in 2003, and mess around with troop deployments in the Gulf region until it was later discovered.

During NATO operations in Yugoslavia, cyberwarriors were deployed to destroy Serbian websites, command and control systems, and they even managed to hack into Slobodan Milosevic's personal bank-account. Hacking can be used by terrorist groups and hostile foreign forces alike, to destroy or create havoc within a country. Most western countries who previously sought to make available information about major public works, such as electricity grids and gas pipelines are now engaged in a process of removing a lot of this information from the public domain.

EMERGING TECHNOLOGIES

What does the immediate future hold for the modern battlefield?

The U.S military over the past 10 years has changed its emphasis from heavy armor and the use of overwhelming numbers of troops in operations, to a lighter, more agile technologically sophisticated one. The *transformational* doctrine espoused by current Pentagon Chief, Donald Rumsfeld has come to mean that new technologies such as laser designators can limit the amount of troops needed upon the ground; the remaining troops being fast moving, deployed in fast moving vehicles and can selectively strike at vital weaknesses in the opposition with added air support. Another area of improvement has been the integration of communications structures into a centralized system. Many countries around the world (South Korea, Libya, Syria) look on anxiously to see the outcome of the Iraq invasion to see if it proves ultimately effective.

Currently, a major push in designing such systems is the ability to wage *virtual war* on high spec computers, modeling real life situations and observing for any potential weaknesses in prototype technology.

Other areas of development are…

- Battle bugs: a small insect like robot mine, that roams the battlefield seeking out a soldiers body heat
- Superbugs: Viruses tailored towards genetic dispositions of some races
- Laser Flashlight: A device that can temporarily or permanently blind a victim
- Polymer Camouflage: The ultimate form of camouflage that acts like a chameleon's skin – imitating the surrounds
- Nanotechnology: Microscopic machines that will detect and repair skin, or armor
- Solar Paneled Clothing: For use in keeping equipment charged and at the ready

GUIDE TO MODERN MILITARY EQUIPMENT

TANKS

The phrase main battle tank or MBT refers to the three vital statistics an army is looking for in their frontline tanks; being the ability to traverse difficult terrain with speed, a high velocity cannon and the ability to withstand impact from powerful missiles and warheads.

The following six tanks meet such demands…

Leclerc – The French Leclerc has an unusual three-man crew setup (the traditional fourth crew-member is now an auto-loader). The tank has a low battlefield silhouette; it also has a detachable, modular armor suite (allowing for upgrades as technology improves). Firepower is a 120mm smoothbore cannon.

Hard Cover 4 Protection Armor Rating 140 (F60 B30 S25)

Leopard 2 – The German produced Leopard has a high power-to-weight ratio (important for transport requirements). It also has a 120mm smoothbore cannon, advanced fire control and special armor laminates (adding to the ability to withstand HEAT missiles).

Hard Cover 4 Protection Armor Rating 140 (F60 B30 S25)

Merkava 3 – The Israeli tank has a unique configuration with a front-mounted engine (designed to help the crew from frontal attacks). The tank is fitted with replaceable modular armor. The Merkava has an advanced *hunter-killer* fire control system. It has a 120mm smoothbore cannon.

Hard Cover 4 Protection Armor Rating 165 (F75 B30 S30)

T-80 - The Russian made T-80 has a compact low silhouette and a three-man crew configuration (auto-loader capabilities). It is pretty mobile and the armor protection is reasonable. It has a 125mm cannon with a basic fire control system. It does however have the ability to also fire tube-launched missiles (for long distance sniping).

Hard Cover 4 Protection Armor Rating 130 (F50 B30 S25)

Challenger 2 – This British made Challenger tank has excellent armor protection (using sophisticated Chobham armor). Its firepower is a 120mm rifled cannon. Its firepower and survivability is at the expense of a low power-to-weight ratio.

Hard Cover 5 Protection Armor Rating 190 (F80 B40 S35)

M1A2 Abrams – The United States Abrams has a turbine engine giving it the edge in mobility, however, it does use large stores of fuel to achieve this. Firepower is a 120mm smoothbore cannon; it has sophisticated electronic fire control systems. Armored protection is provided by Chobham armor (the best currently available).

Hard Cover 4 Protection Armor Rating 175 (F75 B30 S35)

HELICOPTERS

AH-64D Longbow Apache
Max Speed: 162mph
Ceiling: 12,480ft
Armaments: 16 Hellfire missiles and 30mm chain gun

The world's most advanced attack helicopter is deployed by the US and British forces. It has a distinctive appearance, with a mast-mounted radar (that forms part of an integrated fire control radar and missile system). Such systems can target hostile forces through smoke, rain or fog. The helicopter is agile enough to support troops in urban environments.

Hard Cover 3 Protection Armor Rating 100 (F20 B15 S15 U25 T10)

SH60 Blackhawk Helicopter
Manufacturer: Sikorsky
Rotor Length: 16.2m Total Length: 15.3m
Height: 5.1m Weight: 10,650kg
Maximum Payload: 8,350kg
Range: 1630km Max Speed: 360km/h

These medium range helicopters were part of the U.S Armed Forces strategic plan in the 1980s, despite being superceded in the last 10 years they have found their place among some of America's allies defensive capabilities – like Israel and Australia.

Hard Cover 3 Protection Armor Rating 80 (F20 B10 S10 U25 T05)

Chinook
Manufacturer: Boeing
Turbo-shafts Length: 15.54m
Weight: 22,680kgs Height: 5.68m
Max Speed: 298 kms per hour
Range: 370 kms

The Boeing Vertol CH-47D Chinook was first delivered to the US Army in 1962, it is mainly used today to move heavy logistics and assault troop transportation. It is also used by special-forces for insertion, extraction and parachuting. The Chinook can carry up to 44 soldiers and can lift 12 tonnes of stores. New instruments have been fitted to allow for Chinooks to be used at night and in bad weather. The latest version is the MH-47

Hard Cover 3 Protection Armor Rating 95 (F20 B15 S15 U20 T10)

Huey – UH-1H Iroquois
Manufacturer: Bell Huey
Length: 12.77m Height: 4.41m
Weight: 2,363kg
Max Speed: 205 kms per hour
Range: 800 kms

Bell Huey first delivered this helicopter for service to the US Army in 1959 and is most remembered for its activities in supporting troops in Vietnam. It has a distinctive rotor-chopping sound and is able to take a great deal punishment in battle. It has double doors on either side and allow for six men to repel from a hover position rapidly. The *Huey* officially called the Utility Helicopter 1 is still in active service widely around the world today

Hard Cover 3 Protection Armor Rating 80 (F15 B15 S15 U15 T05)

Puma
Length: 16.80m Height: 4.60m
Weight: 4,760kg
Speed: 327km/h

Designed in the mid-1960s to meet French Army needs for a new medium-lift transport helicopter, the Aerospatiale Puma has been adopted by the British and produced at Westland for all-weather day and night tactical transport. Used primarily for transport, the Puma can carry up to 16 fully equipped men or 20 men in light fatigues

Hard Cover 3 Protection Armor Rating 75 (F15 B15 S15 U10 T05)

Sea King Helicopter
Length: 33.15m Height: 5.13m
Weight: 2,451kg
Speed: 215km/h
Range: 1,400kms

The Sea King manufactured by the GKN Westland factory for British service in 1959 has proved a sturdy and reliable helicopter. The Royal Navy utilize the Sea King in anti-submarine operations with a range of over 1,400kms. In emergency situations they can evacuate 42 troops, although the normal load is more like 28 fully equipped marines. It has a payload capacity of 1,633kg (that maybe underslung from the craft)

Hard Cover 3 Protection Armor Rating 80 (F15 B15 S15 U15 T05)

PLANES

F-15 Eagle
Manufacturer: McDonnel Douglas Corp
Wingspan: 13.06m
Take-off Weight: 36,000kgs
Max Speed: Mach 2.5 plus
Range: 5,500 kms

The air superiority of this frontline combat aircraft is achieved by a mix of maneuverability and acceleration, range, weapons and avionics. Its multimission avionics system sets the F-15 apart from other fighter aircraft. It includes a head-up display, advanced radar, inertial navigation system, flight instruments, UHF communications, tactical navigation system and instrument landing system. It also has an internally mounted, tactical electronic-warfare system, "identification friend or foe" system, electronic countermeasures set and a central digital computer.

Hard Cover 3 Protection Armor Rating 100 (F20 B15 S15 U25 T10)

Harrier Jump Jet
Max Speed: 1065km/h

The Harrier family of jets has had long service with the British Royal Navy and RAF. The Harrier's Vertical/Short Take-Off and Landing (V/STOL) capability means it can operate from conventional bases, temporary sites and a wide range of surface vessels (ships etc). The GR7 variant has a full night attack capability, while the Sea Harrier's Blue Vixen radar allows it to use AMRAAM and Sidewinder missiles for air defense, and Sea Eagle anti-ship missiles

Hard Cover 3 Protection Armor Rating 100 (F20 B15 S15 U25 T10)

C-130 Hercules
Manufacturer: Lockheed
Wingspan: 40.41m
Take-off Weight: 70,310kgs
Max Speed: 614 kmph
Range: 7,840 kms

The American C-130 Hercules came into production in 1955 and has been a stalwart of the transportation needs of US forces. It is one of the world's most popular aircraft for lifting medium sized deliveries. They are used also for dropping troops in HALO and HAHO parachute drops. Part of their appeal has always been the Hercules ability use relatively short runaways, and the 100 different types of models produced over the years.

Hard Cover 3 Protection Armor Rating 120 (F25 B20 S15 U35 T10)

F-18 Hornet
Manufacturer: McDonnel Douglas Corp
Wingspan: 13.5m
Take-off Weight: 23,500kgs
Max Speed: Mach 1.7+ plus
Range: 2,500 kms

The F/A-18 Hornet is an all-weather aircraft, it is used as an attack aircraft as well as a fighter. In its fighter mode, the F/A-18 is primarily used as a fighter escort and for fleet air defense; in its attack mode, it is used for force projection, interdiction and close and deep air support.

Hard Cover 3 Protection Armor Rating 100 (F20 B15 S15 U25 T10)

F-117 Nighthawk
Manufacturer: Lockheed Aero Systems
Wingspan: 13.3m
Take-off Weight: 23,625kgs
Max Speed: High Subsonic
Range: Unlimited with refueling

The unique design of the single-seat F-117A provides exceptional combat capabilities. About the size of an F-15 Eagle, the twin-engine aircraft is powered by two General Electric F404 turbofan engines and has quadruple redundant fly-by-wire flight controls. Air refuelable, it supports worldwide commitments and adds to the deterrent strength of the U.S. military forces.

Hard Cover 3 Protection Armor Rating 100 (F20 B15 S15 U25 T10)

B-2 Spirit Stealth Bomber
Manufacturer: Northrop B2 Division
Wingspan: 52.12m
Take-off Weight: 150,635kgs
Max Speed: High Subsonic
Range: Intercontinental

The B-2 provides the penetrating flexibility and effectiveness inherent in manned bombers. Its low-observable, or "stealth," characteristics gives it the unique ability to penetrate an enemy's most sophisticated defenses and threaten its most-valued, and heavily defended, targets.

The revolutionary blending of low-observable technologies with high aerodynamic efficiency and large payload gives the B-2 important advantages over existing bombers. Its low-observability provides it greater freedom of action at high altitudes, thus increasing its range and a better field of view for the aircraft's sensors. Its unrefueled range is approximately 9,600 kilometers. The B-2's low observability is derived from a combination of reduced infrared, acoustic, electromagnetic, visual and radar signatures. These signatures make it difficult for sophisticated defensive systems to detect, track and engage the B-2. Many aspects of the low-observability process remain classified; however, the B-2's composite materials, special coatings and flying-wing design all contribute to its "stealthiness."

The B-2 has a crew of two pilots, an aircraft commander in the left seat and mission commander in the right, compared to the B-1B's crew of four and the B-52's crew of five.

Hard Cover 3 Protection Armor Rating 110 (F20 B20 S20 U20 T10)

Tornado
Max Speed: 800 knots
Length: 17.2m
Weight: 14,500kg
Range: 400 miles

This two-seater, all weather, multi role combat aircraft is in use by UK, Germany, Italy and Saudi Arabia. There are several variants to the basic design, such as the GR18 (enhanced maritime attack capabilities). The Tornado Air Defense Variant (ADV) was developed in the UK to act as a long-range, long-endurance fighter interceptor. Its interception radar has a long-range capability, allowing targets to be engaged from beyond visual range

Hard Cover 3 Protection Armor Rating 100 (F20 B15 S15 U25 T10)

LAND TRANSPORT

Fast Attack Vehicles (Light Strike Vehicles)
Length: 3.9m Width: 1.86m
Height: 1.73m Weight: 1,100kms

Light Strike Vehicles are platforms capable of delivering 2 to 3 soldiers to a destination with speed and allowing for some personal protection. Typically stripped of their exterior paneling they resemble a close approximation of elongated beach buggies Successfully used by US forces in the Gulf War and beyond, they allow for .50 caliber machine guns and grenade launchers to be attached to the frame. There is room for stowage needs, and the water-cooled petrol engine or 4 cylinder water-cooled, turbo-charged diesel engines provide maximum performance output. The vehicles have Kelvar armor, and ignition retardant fuel tanks. Such vehicles can be delivered within 50km of the destination by cargo planes, allowing for special operations teams to drive quickly to their target

Hard Cover 2 Protection Armor Rating 50 (F20 B10 S10)

Hummer
Manufacturer: AM General
Top Speed: 100km/h
Length: Variable
Height: Variable

The nature of the American produced Hummer (an abbreviation derived from High Mobility Multipurpose Wheeled Vehicle or HMMWV) is a compromise to deliver a vehicle that has mobility and flexibility, but also sturdy. Trucks being too bulky and jeeps not being able too fully meet the mid-range stowage needs of troops. AM General developed this compromise in 1981 and it has been wildly successful (with over 150,000 vehicles developed for the US Armed Forces alone). They also produce a civilian version. The Hummer can be converted to support a number of different platform roles. The Non Armored Open Platform, provides for LRRP missions, which can be equipped with a light machine gun and MK19 grenade launcher. The ATGM (Anti-Tank Gun Mount) mounted platform, such as a tow rocket. A closed fully armored platform, equipped with light machines guns to perform border and urban patrols in hostile areas. The Hummer Truck Platform for transportation of equipment to combat zones. The Observation platform for telescopic mounts and electronic intelligence gathering operations

Hard Cover 3 Protection Armor Rating 65 (F20 B15 S15)

Land Rover
Length: 4.5m Width: 1.89m
Weight: 3,400kg
Engine: 3.5 litre V8 Diesel

The ever reliable land rover has been used by armies since the Second World War, it is adaptable to different terrain types and can carry a good payload. The model generally employed these days is the Land Rover 110, which has been modified to hold extra stowage and weapon mounts, and/or smoke dischargers mounted on front and rear. Such platforms can carry Milan missiles, grenade launchers or heavy machine guns

Hard Cover 2 Protection Armor Rating 60 (F20 B10 S15)

ATTACK BOATS

Rigid Raider
Length: 5.82m Beam: 2.2m
Draught: 450m Weight: 360kg
Speed: 37 knots *with 140hp engine fitted*

This assault craft is used by the British SAS and is made from glass reinforced plastic (GRP). The boat has a steeply raked flat bow, making it possible to be driven straight up onto beaches. It has four lift points to allow for helicopter recovery. It can carry nine fully-equipped soldiers with a coxswain. Such vehicles are virtually impossible to sink (mainly because of the specialized fiber used)

Hard Cover 1 Protection Armor Rating 60 (F20 B10 S10 U10)

Rigid Hulled Inflatable Boat
Manufacturer: Morena
Length: 13 meters
Speed: 45 knots
Range: 200 miles
Crew: 3 crew + 8 passengers

The Morena RHIB is currently being used by the US Navy Seals and Shayetet 13 in Israel as a more fixed water platform for rapid ship-to-shore insertion/extraction. This version is much quieter and faster than similar boats, it has ample armaments with two fixed gun mounts holding machine guns and MK19 grenade launchers attached. The hull construction has the ability to take a great deal of gunfire, before deflating

Hard Cover 2 Protection Armor Rating 80 (F15 B15 S15 U20)

11. THE LABORATORY

ADVANCED HACKING PROCEDURES

CYBER-CRIME

A small but dedicated community on the internet (and various other incarnations of computer networks worldwide; including intranets) have dedicated their time to seeking access to restricted areas of private computer servers. Some choose to pursue this activity purely for the intellectual challenge, some do it to maintain the security of their sites as paid I.T consultants, others choose to do it for illegal financial gain. The last category falls into the realm of cyber-crime; that being, any access to secure information networks for the purposes of altering details, selling private information to competitors, destroying information or computer infrastructure, or releasing computer programs (virus, et al) with the intent of causing disruption to services (usually causing a loss of man hours + expenditure). Even if the intent isn't directly correlated to causing such outcomes, it is still illegal in most countries to access secured information, with laws generally holding the hacker responsible for their consequences.

Most policing organizations and Intelligence agencies now have dedicated teams of officers assigned to prevent and prosecute such hackers. It has slowly become acknowledged that such activities have the real potential to cause disruption in our modern telecommunication dependant world. Most critical public utilities such as water, power grids and transport systems; such as air traffic control rely upon some level of electronic control to maintain the service – any electronic system is susceptible to cyber attack.

SMALL TIME HACKING

On the internet, most major commercial, government and educational sites regularly receive some level of attack by hackers. Indeed, the Pentagon regularly receives 10,000+ such *pings* a week. At the lowest level of technique; a hacker can attempt to gain access a secured network by trying to guess a user name and password of a user by *sheer hit a miss* tactics, or by attempting to guess network address extensions, or attempting to use *social engineering* techniques to persuade a person of authority to grant them access, or to send communications with a virus or Trojan horse to a known email address (once the email is opened, potentially an extra executable file is also automatically opened and a virus program is downloaded to the target's computer or server - this seeks to dismantle the electronic security and/or gives the hacker external control over the target computer).

Social Engineering is a term derived from the activity known as *phreaking*, during the 1970s some technically minded individuals like the infamous *Captain Crunch* chose to devote their time to breaking into secure telephone systems to make free calls – this can be seen as an early incarnation of hacking. Social engineering is the term derived from their efforts for misrepresenting themselves to telephone service representatives to gain further technical information about the particular network they sought to *phreak*.

INTERMEDIATE HACKING

Most intermediate hackers realize pretty quickly that such hit and miss tactics are a vast waste of their time and effort (and they are easily tracked backed to their I.P address). They usually seek out communities of hackers online, and gain access to information and existing hacking tools (software and hardware). The abiding concept generally starts to become clear - you need software that automatically pre-generates passwords, you need a *lot* of computing power and you need fast internet access and the ability to disguise your identity. Add to this, the general accumulation of knowledge of potential *backdoor* opportunities for some servers and software tools gathered from other hackers – the hacker quickly becomes a far more potent and resourceful opponent.

ADVANCED HACKING

NETWORKING

The experienced hacker would never choose to access a target site directly.

Hacker's Computer -> Communications Network -> Target Computer

Instead, the hacker would seek to redirect their activities through intermediaries; such as a re-mailer service, or through a string of poorly secured home computers, or through the use of a laptop through a remote access point (hotel phone-line, satellite-phone or microwave access, or indeed, tapping into a neighbors telephone line). It is readily apparent to any I.T professional that major business software applications are not as secure as the novice user might suspect (*…here's looking at you Mr.Gates*); it is possible for an intermediate hacker to install *spyware* on one's home/business computer and take control of that system in a matter of minutes. Most experienced hackers would generally avoid such obvious intrusion (as being counter-productive to their aims), they would only need to use a small fraction of a computer's power to perform their activities (see example below).

Hacker's Computer –> Slave Computer 1 –> Slave Computer 2 –> Target Computer

Once you have performed this simple task over and over again, say into the thousands of linked computers, it would generally make it *very* hard for anyone to track the source of the transmissions; add to this, any decent hacker would also have software prepared in advance to remove any trace of the computer *logs* once the desired access has been achieved (slowly sending pings to exit each computer back to source). You will understand that catching such a good hacker generally comes down to luck (or by the hacker being less than cautious in bragging to fellow hackers).

ZOMBIES!

Another advanced hacking technique is the use of *zombie* computers; essentially this is exactly the same process as taking control above, but by using a number of computers to simultaneously ping the same server. Instead of sending each potential password one-by-one, the enslaved computers are configured to send multiple hits at the same time. The advantage being it gives little time for counter-measures to close down the access, and it multiplies the potential suspects of the original transmission (hindering attempts to quickly find the hacker before he changes the data logs).

If you successfully combine both networking skills with enslaving other computers, it is literally impossible to catch such a hacker by conventional means (most hackers get caught by their own ineptitude, hacking sites beyond their current abilities, or bragging to fellow hackers). The best investigators can usually do is to target individuals by their basic behavioral/ideological traits.

THE ENEMY WITHIN

It is rare for experienced hackers to bring down sites or to take complete remote control over it's server, why do so? And for what expressed purpose? In most scenarios the hacker will find a way into a server, create a backdoor and disguise it and leave (or if vindictive, leave behind Trojans horses + logic bombs). At a later date, they can return when the alarm has died down, gain access to vital security information and legitimate their continued access. They can achieve their aims safe in the knowledge that not only do they have current information but; they will have continued access (and potential control) into the near future.

CYBER WARFARE

In the world of economic espionage, intelligence and terrorist activities, a new battlefield has emerged, that of cyber warfare. With the growth of alternative forms of computer media (blogs, alternate news websites, satellite phones et al) it is often necessary for governments to try to limit the news access to alternate points of view. During the bombings in Bosnia and Iraq, online radio stations and blogs provided alternate pictures of the effects of *smart bombs* going off course - hardly being the wonders of modern warfare as espoused by military experts and main-stream media alike (U.S military figures from the first Gulf War in 1991 give an accuracy rating of 85% for smart bomb technology – although a healthy rate, media coverage suggested virtual infallibility).

If you take the time to navigate around the web, you will also find websites devoted to the ideology of terrorist organizations. If all politics comes down to ideology, who that controls the medium of exchange can also dictate policy.

Cyber warfare also represents the efforts to find data from online government resources; open source information is often a lot more reliable than human intelligence. Also, with the growth of electronic command and control systems in modern armies, attempting to gain access to these secured networks can greatly enhance one's side chances winning.

ECHELON & OTHER SYSTEMS

In the world of Signals Intelligence a revolution has been slowly taking place over the past 20 years. The days of physically bugging telephones is nearly ended. Today around the world some 50 countries partake in advanced forms of electronic capture of the world's telecommunication signals via ground bases, satellites and air reconnaissance (such as UAVs). The United States and a select number of allies have developed their own response called Echelon, a sophisticated computer program that uses keywords to scan vast amounts of captured telecommunications from a multinational collective of satellites.

The system has grown out of the UKUSA agreement established between the partners after the Second World War to share greater levels of information. The major partner in this arrangement is the United States, which retains overall control over the system via the National Security Agency (NSA); it develops the system and effectively runs it. The United Kingdom is a major partner and runs its stations through the Government Communications Head-Quarters (GCHQ) agency. In the 1990s three more partners were introduced to the arrangement as somewhat junior partners – Australia (Defense Signals Directorate DSE), Canada (Communications Security Establishment CSE) and New Zealand (Government Communications and Security Bureau GCSB).

The system primary uses its collective of Intersat satellites, which sit in geostationary orbit over the equator, which captures all forms of international telecommunications (fax, computer, phone, satellite phones, connected automated linked computer terminals etc). Another primary source of information is tapping into the world system of Inmarsat-2 satellite dishes, which are primarily used as the backbone of mobile phone technology networks. The U.S also uses the Echelon network to sort through data from its movable military spy satellite systems (which obviously, it doesn't share with its partners). The Menwith Hill site in the United Kingdom virtually taps directly into the nearby British Telecom's microwave network (which was purposely designed to converge on Hunter's Stone junction tower). Civil libertarians decree such purposeful implementation (along with SystemX which allows direct tapping of British Telecom telecommunications network by the Government) seriously infringes upon civil rights.

Other ways in which information is gathered is by tapping into under-ocean cables, using embassies to tap into short wave radio transmissions (HF radio, military radios, walkie-talkies) – the first two are only line of sight devices, that cannot be picked up from satellites. There are boats fitted for surveillance sent in near trouble zones, UAVs and specialized high flight planes to monitor sensitive areas.

One way or another all these sources are fed into the Echelon network, where the data is collected and processed. Each station has a dictionary of *keywords* fed into the system by each agency, once the data has been checked reports are sent out to the appropriate agency. The overall control of the system is maintained by the NSA, it primarily funds the expansion of the bases and has ultimate say on the information its partners get to see. The basic arrangement *is we pay for, we decide what we supply you with*. There are indeed many takers; recently some 10 even-junior partners have signed up for the service including Norway and South Korea.

The current stations include the following…

NSA Sugar Grove
CSOS-NSA Morwenstow, United Kingdom
CSOS Stanley Bay Hong Kong
NSA Yakima, Washington State

These four stations are the major relay stations and pick-up stations for Intersat transmissions

NSA Menwith Hill, United Kingdom
CIA Pine Gap Alice Springs, Australia

These two stations primarily handle the US spy satellite transmissions and the results are sent to Fort Meade, Maryland (main NSA operations center)

GCSB Waihopai New Zealand
DSD Geraldton, West Australia
CSOS Two Boats Ascension Island
Misawa, Japan
Sabana Seca, Puerto Rico
NSA Buckley Field, United States

These auxiliary stations feed into the main system

ECONOMIC INTELLIGENCE

The system is a supremely powerful tool that is the envy on many nations around the world, although Echelon was set up to gather diplomatic and intelligence needs, it equally serves the interest of United States businesses. With the system picking up the vast quantity of the world's communications, small snippets of business information are routinely picked up. The United States has been accused of using the network to its own economic advantage by looking after its key business interests (oil, military and scientific development). The European Parliament conducted an Echelon Commission of Enquiry in 2000/01 to decide on the European stance to such broad ranging surveillance issues, concerning its citizens and European business interests.

One such abuse of power is taken from a French spy satellite initiative in 1982, an Indian military contract was up for renewal on military planes, the French Economic & Technological Intelligence division of the DGSE handed Dassault Aviation (a French company) quotes of competing American and Russian firms. It was then a simple case of the negotiator making the appropriate bid to beat out the competition.

Critics have suggested the United States is creating an unfair playing field for business with such access to private telecommunications, and doubt that the US activity gives its partners access to uncensored information. Yet; the US keeps adding members to Echelon's list of partners (primarily to stop these nations developing their own comparative networks).

Of major concern to civil libertarians is the complicity shown by the partner organizations, whereby the partners agree to spy on local civilians – most of the countries involved have laws against such intelligence agencies spying upon their *own* citizens without authority. One such case is alleged to have taken place in the 1980s whereby Margaret Thatcher regularly received updates about fellow government ministers via Canada's CSE. Some may speculate that such activities are necessary to combat the new quantum magnitude of terrorism, others would argue this is an outrageous abuse of government power.

The only problematic area for Echelon's reach is fiber optic cabling, which is generally buried underground. With its growth in usage, it presents a challenge to the supremacy of the system. Finally, despite the unrivalled ability to capture data, it still requires vast computer and man-hours to sought the information, limiting notions of *Big Brother* like behavior.

OTHER SYSTEMS

Around the world, many other countries have their own resources to call upon to provide them with information. The French use their various colonies around the world to play host to their own radio satellite bases (such as New Caledonia); Germany also has a vast number of bases around the world. Latterly, Japan has developed its own network. It would be wrong to surmise countries outside of the Echelon partnership program do not have access to electronic information gathering capabilities (it is relatively easy to pick up the world's microwave signals). Besides, a lot of information has always been exchanges readily between friendly and not so friendly countries – if it isn't directly valuable.

FORENSICS

As popularized by television series such as the *Crime Scene Investigations* (C.S.I) franchise, the art of forensics in reality is a conglomerate of scientific studies. Internal intelligence agencies (such as the F.B.I) usually have a number of specialist divisions devoted to *forensic science*, or the pursuit of science applied to answering legal questions (criminalistics being the process of scientific collection and examination of physical evidence, which is the sub-branch popularized by police investigation type shows).

THE CRIME SCENE

The standard procedure undertaken by most trained police officers at a crime scene is to generally check if the victim is still alive (resuscitate if so), clear the area of people, gather the personal details of as many eye-witnesses as possible, find if anyone has removed items from the crime scene (or moved the body), make sure not to touch anything unnecessarily, and to wait for the specialist units to arrive. Of course, in reality, a crime scene is sometimes in a state of pandemonium, a veritable media circus in fact - meaning there are factors that invariably contaminate a crime scene picture. Once the perimeter tape is up, the detectives will usually arrive.

DETECTIVES

The work performed at the crime scene is actually quite mundane, but essential. Once the detectives arrive the major concern is making sure useful records are created and the establishment of a *chain of custody* for evidence, that being, making sure that all evidence maintains its credibility in the eyes of the law. So this entails creating photographic records of the body position, shooting close up shots of any evidence gathered. The detective will also observe and note if the lights were on, windows and doors were locked or open, the points of trajectory of bullets and looking for any fingerprints. Evidence is carefully bagged, swabbed or eye-dropped into sterile containers.

(FORENSIC) SEROLOGY

Forensic Serology is the study of blood and other body fluids in relation to a crime scene reconstruction. After death, the body tends to break down in a basic set pattern. Approximately 30 minutes after death the blood vessels tend to relax (post-mortem lividity), and the blood will press downwards because of gravity, meaning the lower side of the body develops a distinctive purple hue to the skin. Up to around 8 hours, if an investigator presses this flesh (or the body is moved) the blood will blanch, that is the blood will flow away if the skin is pinched and gradually return. After 8 to 10 hours, this blood becomes fixed in place (fixed lividity). After about 4 hours rigor mortis starts to take place, the smallest muscles (eyelids, face and lower jaw) will start to shorten, gradually spreading to the rest of the body. Finally, after around 48 to 60 hours the muscles will generally start to relax again, as the cells start to break down (cell decomposition). Armed with an understanding of this process, an experienced detective should be able to establish the time of death with some certainty (at least for the recently departed).

Once in the laboratory, one can start to look at any blood, spittle, saliva, sweat, semen or urine. Such investigations might be useful in finding out the identity and method of death of the victim, but it might equally point the way to finding the perpetrator – as generally speaking, most victims tend to fight off their attackers in some capacity; usually in the exchange, fluids are spilt or the attacker is scratched, leaving skin deposits under the victim's fingernails.

If blood is recovered, tests can be run to identify the enzyme phosphoglucomutase or PGM, there have been 10 different types identified over time, so with careful marking and comparison, 3 or 4 matches correlates to reducing the probability of the suspect down to roughly one in a million.

(FORENSICS) ENTOMOLOGY

Forensic Entomology is the study of insects associated with death. The science has built up considerable case study records to help establish relative times of death by the activities of insects upon (within) the corpse.

10 minutes
Flies will start to lay thousands of eggs in the mouth, nose and eyes

12 hours
The eggs start to hatch and maggots start to feast

24-36 hours
Beetles arrive and start eating the dried skin

48 hours
Spiders, mites, millipedes arrive to feed on beetles and bugs

The actual decay of a corpse can also be slowed (cold) or speeded up (hot) by prevailing weather conditions. One can also observe useful information by looking for any build-up of bugs in a particular areas - as an infestation around, say the hands, might indicate an obvious entry point for insects – because the victim may have fought off their attacker or had tight bonds around their wrists (potentially ruling out natural death claims).

MEDICOLEGAL AUTOPSY

The Coroner will order a medicolegal autopsy if legal justice is dependant upon finding out the cause of death. Firstly, the individual charged with performing the autopsy will visit the crime scene. The autopsy will then take place, present will be either a pathologist or medical examiner (or both) and a police officer. Everything is measured, detailed and photographed to ensure no foul play. There will be identification of the body, then a detailed examination of the body will seek to find any scars, markings, bullet-holes or bruising on the outside of the body. Then, the body is opened up and the internal organs are removed, weighed and observed. Finally toxicological tests will take place on the body fluids and organs to identify any drugs, alcohol or poisons present in the system.

Common activities during an autopsy may include; scraping under the fingernails for material (the victim might have the attacker's skin cells under their nails from fighting back), looking for petechiae, that being pinpoint haemorrhages around the eyes possibility indicating asphyxiation, siphoning body fluids including urine, checking the genitalia and swabbing for any signs of sexual violation.

It may be necessary to perform some reconstructive work on the fingers (for fingerprinting) by the injection of fluid (dehydration), or the removal of fingers and rolling the skin for *floaters* (drowned corpses). The teeth might be reconstructed, or examined using forensic ondontology, detailing any bruising that might match bruising on a suspect. Forensic toxicologists will examine the fluids attempting to detect sufficient levels of compounds that may have led to death.

FORENSIC ANTHROPOLOGY

Often corpses are recovered months or years later, in advanced stages of decay; often the only way to tell information about the victim is by the skeleton. Careful observation may find a particular cause of death (nick or blow on the bone mass), the sex and age of victim (shape of pelvis and jawbone and the sutures in the skull – as we age the skull becomes a fused mass) and illness or poison (deformities to the skeleton and some poisons can remain in the marrow structure of bones after death). One can also tell handedness, because we generally have longer bones in that limb. One can generally tell the race of the individual through statistical variance tables, and some occupations wear some bones out more readily. Finally, one can carbon date bones and reconstruct vague facial features to help with identification.

FORENSICS BALLISTICS

Forensic Ballistics is the study of firearms in relation to crimes. Your average gun (except shotgun) is rifled, that is the inside length of the barrel has grooves in a spiraling pattern to promote a spinning motion that helps the bullet travel smoothly and accurately. Your average live ammunition (cartridge) consists of a projectile, primer, gunpowder and cartridge case. The firing pin hits the primer and the gunpowder inside explodes, sending the bullet out through the end of the barrel. Along the way, however, various imperfections of the rifling on the barrel will imprint itself as it passes along the *land* (raised set of grooves). If a gun is recovered at a crime scene or a suspect's home, test firing can occur in a lab to see if the striations are similar to those on the bullets recovered from the crime-scene (the gun is fired into a water container). Other forensics tips include; blowback can occur during firing leading to various incriminating fibers potentially being sucked back into the gun chamber, a gunpowder burn might imbed particles in-between the suspect's thumb and finger where they allegedly held the gun. One can also determine the angle and distance of the trajectory by performing a gunshot residue test (G.R.S), the traces of metal embedded around the impact zone mean that if someone has fired at distance, there is a larger pattern of tattooing and stippling. Burn marks on the furniture and gunpowder on the floor may also give away the direction of firing. One can even use a piece of doweling to help establish the trajectory of a bullet.

Important information may even be gleamed by close chemical inspection of the bullet, as it may have passed through other victims in flight. Finally, there is a misconception that glass breaks easily in Hollywood films. Glass is a liquid, when a bullet passes through a window, its elastic properties generally mean it will pass through it with minimum resistance and damage. When the bullet has gone through, the glass reflexes and deposits the shards of broken window on the *same* side the bullet came from – which is helpful in trajectory analysis. In modern times, laser pens and computer modeling programs are tremendously helpful in determining various crime scene pictures.

FIBERS

When individuals are involved in a struggle, or even just visiting a location, they tend to leave behind hair, dead skin cells, and clothing fibers as a matter of course. These may be useful in establishing the suspect was at the scene of the crime.

CAR PAINT & OTHER MATERIALS

One may also be able to work out the car the attacker drove away in if they hit something en-route, most police agencies have complete records of paint samples of all cars produced within its country, so it may be possible to match them by batch. Images of car tires are also kept on file by most police agencies for reference, most car tires end up with slight imperfections in their grooving during manufacture and wear, this can become a vital piece of evidence for matching vehicles to crime scenes.

MASS SPECTROMETER

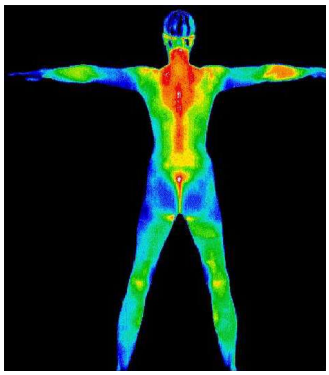
Using a mass spectrometer an investigator can break down any compound into its constituent substances, by carefully cross-linking the percentages of each substance present within the record, no matter whether it is blood, soil samples or car paint chips - the sample can be matched to a potential identity, location or manufacturer.

IMPRESSIONS EVIDENCE

Fingerprints are a ready source of clues at most crime scenes; they may either be plastic prints (impressions left in pliable surfaces, like putty), visible prints (fingerprints smeared in blood or ink), or latent prints (invisible to the naked eye). There are many ways to detect such prints; like the use of a laser pointer, ultraviolet light rod with powder, or using agents such as ninhydrin or silver nitrate – that react with fatty amino acids in the print. Once obtained the prints can be digitized and compared with police fingerprint databases; looking closely at the various arches, whorls and loops present on the specimen.

Footprints at the scene of a crime can be photographed and compared with databases of various common brands, hopefully, narrowing down the suspect apparel. The image can be magnified further to see if there are any telltale scratches, cuts or areas of wear present. An impression maybe taken of the ground, named a *moulage* (plaster cast). Finally, a device can be fabricated out of foil and a high voltage source that can be charged over a dusty footprint, and use of an electrostatic charge can *lift* the footprint for evidence.

A common sight at the scene of a crime is an improvised weapon, like a household tool. One can make comparisons between the entry wound on the victim compared to various case records of such attacks to make a positive match. Also, one can carefully attempt to match any metal shards present within the wound with the suspected murder weapon.



DNA FINGERPRINTING

The large growth area in modern forensics has been the use of DNA testing. The process involves extracting DNA from the blood and cutting it up into small strands by the use of chemicals, the strands are then placed in a control agent gel, and then a current is applied. The DNA strands eventually start to react, moving through the gel: and the activities observed lead to classification. Taking into account the varying competing (and contentious) standards applied to this process, it is fair to say the results narrow down the probabilities to 1 in 10,000,000 that the suspect is the criminal.

IMAGING TECHNOLOGIES

A fairly recent advance in computers has been the ability to enhance the detail on a photographic image, using much the same technologies that make JPEG photographs compact, a computer program can manipulate the image by extrapolation of the two pixels, either side of the derived one. Although infinite resolution isn't achievable, using such technology can increase the functional magnification by 4 to 8 times. One can also use computer technology to artificially increase the light source in photographs, although the human eye doesn't pick up the distinction in low-light images, by artificially increasing the level of contrast, some images can be recovered from poorly lit film.

BEHAVIORAL PROFILING

Much has been made of the job of a behavioral profiler in modern fiction, delving into the fields of psychology and crime investigation conjures up the mystic of Sherlock Holmes taking on his Moriarty. However, the truth is somewhat different. The modern profiler is likely to be searching criminal databases like the FBI's Violent Crime Apprehension Program for various similar cases histories, interviewing incarcerated killers, or by reading up psychology textbooks. Through the FBI's program most serial killers have been found to be between the ages of 25 to 35, had mental illness bouts at least once, almost all are men and often had a history of torturing animals or pyromania. From such statistical histories, the art of profiling is often more about dedication than deduction.

RADIOACTIVE DEVICES

The abiding fear of many civil authorities is the use of a nuclear device in one of the world's major cities by terrorists. Although it virtually impossible for a small country, let alone a terrorist organization to start its own nuclear program, it is substantially easier to pay someone to acquire ready made parts and/or a working device.

The fundamental problem of nuclear devices is getting your hands upon enough enriched Uranium (uranium-235), or Plutonium (plutonium-239). These substances go through a complex process of refinement needed to be able to achieve *fission*. Although, weaker grades of enriched plutonium can be achieved by the specific use of industrial centrifuges, it is unlikely to be achieved without a top project manager of considerable experience in the industry.

The second requirement is neutron reflective material (usually comprised of iron, graphite or beryllium). This material is needed to funnel the electron flow to a fissile material, although one can create a bomb without such deflector casing material; it runs a substantial risk of not detonating correctly (although it still functions like a poorly constructed dirty bomb). For a fission bomb (similar to early bombs dropped on Hiroshima in WWII) to achieve nuclear fission, a smaller unit of nuclear material is forced to collide with a larger mass by a conventional explosive.

Generally, the better the quality of the enriched material, the better the chances of achieving fission, and the less material needed (plutonium bombs can be the size of suitcase, whereas enriched uranium bombs generally weight in at a ton).

For a standard nuclear bomb at least 60lb of reactor grade plutonium is needed (less for weapons grade), neutron reflector material, a secure metal casing and at least 1,000 lbs of conventional explosive. To construct one would need considerable knowledge in the nuclear field, or risk creating an expensive dirty bomb. Such a device would have a 1 kiloton blast capacity that would kill people instantly up to a radius of ½ kilometer and spread radioactive material at least up to 3 times that area (depending upon subsequent winds the contamination zone might stretch for tens of kilometers). Your typical Russian made suitcase bomb would have a 0.1 kiloton blast.

The Russians also developed uranium fuel for their naval nuclear submarines, which is produced at higher refinement standards than your standard weapons grade specifications.

Dirty bombs are a lot easier to create, as their main distinguishing feature is they do not reach fission. They are designed to use a conventional explosive to spread highly active radioisotopes over a large area (usually radium or cesium). The initial explosion will cause the same amount of damage as a conventional explosive, but in the area of dispersal, the individuals there will be exposed to radioactive contamination, similar, but lesser to the secondary exposure in a nuclear explosion. The area will subsequently be uninhabitable, unless the topsoil is taken away – as people will continue to take radiation damage.

An incident in the Brazilian city of Goiânas in 1987 serves as a warning of the potential of dirty bombs to cause panic and alarm (and financial pressures on local governments), a local scrap metal merchant stole a small caesium chloride canister and cut it open. The powdery dust drifted off across the city, four people died and 200 were contaminated.

The local community became alarmed and sought reassurance about their own health, 10% of the local community of a million sought radiological screening – hospitals were overwhelmed and citizens protested in the streets. Eventually, 10 football fields of earth (3,000 cubed meters) had to be removed because of contamination over six months. Similar airborne compounds were used in the Soviet Union's farm programs, 7,000 devices were produced to irradiate seeds for production (in the hope of increasing yields).

Another Soviet invention was mobile electricity generators, which were powered by radioactivity (strontium-90); they were produced in there 1,000s. One apparently was at the heart of a scare in Georgia, where 2 woodcutters were exposed to severe radiation burns in woodland – investigators were so concerned in recovering the device they took 40 second shifts to remove the contamination.

The worrying fact is, the type of materials most potent for using in dirty bombs are relatively unsecured in hospitals (cesium isotopes as used in x-rays) and in industrial machinery used worldwide.

THE BLACK MARKET

The International Atomic Energy Agency (IAEA) and the United States Department of Energy have been carefully helping to secure the bulk of the former Soviet Unions vast stockpile of nuclear weapons and fissile materials since the early 1990s. As of the end of 2000, only 40% fissile material has been secured and 60% of weapons have been secured to international standards. In a country where poverty was a way of life for many people after the dramatic shift towards democracy in the early 1990s (even still today), there is a great deal of speculation that the sale of radioactive material on the black market was an option. Indeed, there have been many reported thefts of spent fuel rods from Soviet nuclear stations and other fissile materials – in places like Minsk in Belarus.

The fear is that age-old drug trafficking routes through Kazakhstan, Uzbekistan through to Afghanistan will be used by unscrupulous organized crime groups to on sell old Soviet weapons and fissile materials to radical Islamic groups in Pakistan (despite U.S sponsored radiological scanning devices being sent to border-posts).

There are indeed fears that radical followers of Islam within the Pakistan atomic energy program have been providing their expertise to Usama Bin Laden

EFFECTS OF SECONDARY EXPOSURE TO RADIATION

High Doses: People being exposed to some 4000 to 5000 Rads would suffer Central Nervous System Syndrome; being brain tissue would swell with the radiation damage causing nausea, vomiting, diarrhea and progressive difficulty in walking, talking and thinking clearly. They will start to develop convulsions and pass into a coma (dying within the first or second day of exposure). No treatment would be effective.

Medium Doses: Being exposed to ranges between 400 to 600 Rads would suffer gastrointestinal forms of radiation sickness. They would experience nausea, vomiting, and diarrhea soon after exposure. This would last for a few days, after which time they would seem to improve. However, the symptoms would return more violently within a few days to a week, leading to bloody diarrhea (as the lining of their stomach and intestines damaged by radiation would shed). The majority of these patients would also die despite medical therapy.

Low Doses: People exposed to 100 to 300 Rads would suffer hematologic radiation syndrome. They would also suffer nausea, vomiting and diarrhea for a few days. After three weeks their bone marrow would stop producing normal numbers of blood cells. As their white blood cell count falls, they would become prey to infection. Sores will start to form in their mouths, burns and other wounds will become infected and fail to heal. There would also be a corresponding fall in their platelets in the blood (the cell fragments which help blood to clot) and blood would hemorrhage into their skin, and new bleeding would begin in their intestines and stomach. If they survived these medium term complications, they would have a good chance at survival (although admittedly, with a far greater chance of developing some forms of cancer).

Finally, it is hard for doctors to initially diagnose just how many *Rads* a person has been exposed to (given initial symptoms are fairly similar).

SCENARIOS

The British BBC television series Horizons modeled 2 scenarios of dirty bombs going off near Trafalgar Square in London, and in Washington DC's Underground train network. Plus, a model of a simple nuclear device exploding in Manhattan.

Trafalgar Square Scenario #1

The attack supposes a dirty bomb containing 4.5kgs of Semtex plastic explosive and large caesium chloride radiological source (activity rate:74,000 gigabecquerels). The device is detonated in an open public area.

The blast will kill a handful of people nearby (dependant upon pedestrian traffic). The dust cloud of the bomb will carry the powdery caesium tens of meters into the air. The plume will travel downwind at around 300m per a minute.

Once emergency teams arrive on the scene, it may become apparent that there is radioactivity present. Evacuation of the area will follow without any visible health problems. No one would contract radiation sickness, but the exposure will increase the percentages for dying of cancer at some later stage in life.

Exposure to radiation is measured in sieverts (Sv), the unit of measure takes into account our bodies which vary in susceptibility to alpha, beta and gamma radiation. 1Sv causes radiation sickness, taking 8Sv would kill you outright. The basic natural background level of radiation is roughly 0.002Sv.

In the simulation anyone at a distance of 5km of the blast will receive an additional 0.001Sv (half the background level in excess), increasing their chance of cancer marginally by 0.1%

People at 1km distance sustain a 0.012Sv dose, and increase their chance of cancer by 1%

If one remains within 500m of the Square for an extended time without protection, or regularly comes within 200m of the blast zone for extended everyday travel, they risk 80 times the background dose (0.16Sv) – which is sufficient to cause cancer in 1 in 7 people.

Washington DC Metro Scenario #2

In this fictional scenario a dirty bomb incident, a smaller device is used within a more contained environmental space. The amount of caesium is 74 gigabecquerels (just one thousandth the mass of the London scenario). The amount of explosive is roughly the same amount as within a standard firework.

Detonated in a quite corner of a subway station, the blast is only enough to properly disperse the caesium into the air. Under such circumstances it may go unnoticed, in this scenario 24 hours elapse before it is discovered. In such a timeframe, the packed Washington DC Metro line has thousands of commuters and hundreds of trains will spread the radioactive caesium through the stations, and the wind created by the trains will spread the contamination around the underground network

The health effects will be slight to the general public, statistically increasing their risk of contracting cancer by 1 in 4,000: the Metro staff however, face an increase risk of 1 in 100 after a day of work.

The major concern would be the lack of confidence in the underground network, and the massive clean up bill required.

Manhattan, New York Scenario #3

The nuclear device in this scenario would be the equivalent to the blast that leveled Hiroshima (using some 30 pounds of uranium), it wouldn't necessarily have to be on land (it could be detonated remotely by wireless/mobile phone as a container ship sailed into New York harbor). Although, New York Harbor now has nuclear scanning equipment installed, they only ever scan 2% of shipping crates.

The blast in Manhattan would immediately wipe out 50,000 people and 200,000 people would be exposed to lethal levels of radiation. Such a blast would in all eventuality, empty the city for habitation – meaning millions of inhabitants would fan out across the U.S causing great levels of civic disorder.

The U.S would hopefully get some advanced warning from its intelligence agencies, if so the Nuclear Emergency Search Team (NEST) would be deployed from their base at Maryland covering the city with helicopters, vehicles and briefcases equipped with radiological detection devices to hopefully find the device. It would take at least 2 weeks to check the entirety of the city (unless other agencies were officially warned and enjoined into the process). Such a process was covertly undertaken after September 11, when a FBI informant suggested a nuclear attack was imminent on New York.

Many experts in the field suggest such false alarms hint at the prospect of a major world city eventually succumbing to a radiological attack (either dirty or nuclear).

FORGING FALSE IDENTIFICATION AND DOCUMENTS

Creating a false identity generally requires 2 things – an example of the document to be replicated *and* changes to any official records (computer or written) that corroborate the reproduced document. For all due care and attention paid to the recreation of a driver's license (photo, materials, holographs, fonts) it would prove useless if you were stopped by police - the police would arrest you for providing a false license (after they checked it against the linked traffic authority database).

FORGERY AND ANTI-FORGERY TECHNIQUES

There are a number of ways to ensure an ID is secured against forgery, including

- Embossed Pattern
- Watermarks
- Coloring & Unusual Dyes
- Special Inks
- Holographic Images
- Metallic Foils
- Microscopic Fibers
- Specialized papers or plastic film coatings
- Encrypted Bar-Coding
- Microchips or Smart Card technology
- Radio Transponders

A number of such replication devices are certainly within reach of your average citizen. Color photo I.Ds are easily replicated on a home computer setup, with access to a digital camera and color printer. Laminators can be purchased at office supplies stores. Machines for reproducing watermarks, bar codes, embossment, holograms and magnetic strips can easily be *acquired* from printers, or used after hours by staff – and even obtained on the *grey market*.

Obtaining the right materials for the job is a lot harder than you might imagine, generally the plastics and dyes for driver's licenses and credit cards are produced to measure. Subsequently, one either has to steal such goods from the supplier, or purchase a similar batch (leaving a paper-trail) – both raising suspicion. It is possible to synthesis such materials, however, it does take considerable skill and time.

If one is an official of the government, such necessity to reproduce documents might be obviated by making official requests for such documents to the necessary authorities (and the necessary changes to the official records) – but it will still take some time.

The use of magnetic strips, microchips and radio transponders creates a great deal of complication that most organizations might not have the necessary access to equipment to reproduce, let alone decrypt the data. Being such, it is very unlikely within a campaign environment that advanced forms of magnetic strips, microchips and radio transponders will be recreated successfully.

Of course, any talk of reproducing I.Ds is predicated upon having access to an existing one to replicate.

FALSIFYING RECORDS

Most I.D passes are generally automatically checked off against computer database records, if the false I.D are present, alert measures will be triggered. Traffic control cops invariably check the records of people driving erratically before stopping them, to say nothing of when they seek to charge individuals for misdemeanors – so it is important to do the second step of the process.

There is also the complication that some control systems generally need passwords, keypad codes, voice prints and fingerprints. So it is generally best to gain access to the targets computer systems before any physical infiltration takes place.

There are a number of ways to gain access to identity databases; bribing officials, computer hacking, using less secure remote access, *social-engineering* or threatening the safety of a staff member's family.

Even if you have managed to secure both the documentation and changes to records, it may still be a risk to enter highly-secured locations because of the lack of diversity in staff – you may well be noticed as an outsider.

Examples:

Here are some examples of common falsified documentation from the United States

Birth Certificate: This certificate is generally the building block for developing a rounded alias, and it is handy/necessary for obtaining legitimate forms of documentation like driver's license, passport etc. It is also accepted as proof of citizenship when seeking employment. The Birth Certificate is issued by the local branch of the Bureau of Vital Statistics - it is generally sent out by mail, so one could feasibly intercept or recreate such conditions. Historically, records of children who have died young have been *spoofed* by criminals and intelligence services alike to establish falsified identities – although recent moves to computerization within most agencies has added a level of complication.

Common Access Card: In a recent upgrade of personal security in 2000, the United States started to consolidate all forms of government and military I.Ds into one – the Common Access Card. This multipurpose smartcard has an integrated microprocessor with 32k of memory, two bar codes and magnetic strip. The card has in its memory; a digital photo, name, rank, agency, digital certificates, expiration dates and blood type of the individual.

Driver's License: Although issued separately in different states, these laminated cards generally have the name, photograph, physical descriptors and sometimes residency information of the individual. Most state highway patrol cars in America have access to computers in their vehicles to verify the validity of these licenses – even across state lines.

Death Certificate: The documentation to legally dispose of a body, they are generally issued by funeral homes and doctors.

Government I.D: These laminated plastic cards carry a photo of the individual, agency emblem, identifying number, signature, issuing and expiration dates, and limited personal information. An example of such is the color-coded (green for active service) military I.D (as in the Common Access Card description). The use and scrutiny of such cards is dependant upon the sensitivity of the area one wants to enter. It may also help to incorporate other forms of security clearance into one's cover – like a military security pass for one's car.

Marriage License: Are useful for establishing the undercover credentials for agents posing as partners.

Passport: A passport generally is emblazoned with the embossed symbol of the country of origin of a traveler, visas for travel inside, stamps from previous destinations, photo and limited personal information. Most forged passports are altered stolen passports, and there is a thriving trade worldwide in *cut-outs* for criminal organizations selling them.

Pilot's License: A pilot's license generally consists of a number of documents specifying the types of aircraft the bearer may fly, and whom he/she may carry. In times of heightened civic unrest or war, pilots are also issued with security graded passes to airfields.

Professional License: Generally for Law and Medicine these professional certificates carry heavy punishments for falsification and misuse; two types generally exist, the membership card/certificate of a professional body and the corresponding university degree.

University Degrees: Using the loop-holes within local laws or established in overseas countries, one can purchase a degree from a fictional University for *home-study* for as little as $1,000 dollars. It is also possible to falsify established University degrees for as little as $100.

Vehicle Registration: This piece of paper generally doesn't incorporate any security measures, but a sticker to place on the vehicle window.

Visa: A certificate, stamp or a sticker, which authorizes access to a particular country can be particularly hard to obtain, and prices for such may vary. Places like Russia require an *invitation* to enter (basically requiring a large fee to be paid up front).

Weapons Permit: Such licenses are easily obtainable in the United States after rudimentary criminal checks (varying widely elsewhere), sunset clauses of 48 hours exist in some states. A permit may also require a photograph of the user. Police have access to official records to verify.

Security Passes: Most military or commercial security passes generally specify an area of access, a grade of security clearance and the function of the individual. The granting of access to secure government sites generally has to be obtained through official channels, insiders, or fabricated. The criminal underworld generally has no desire to break into secure government sites, so attempting to purchase such passes off them is somewhat foolhardy.

The Digital Trail: Often in setting up an alias/legend it may also be necessary to set up a basic online presence, a lot of information can be gleamed online about even the most ardent Luddite if you know where to look. Increasingly business groups (banks, grocery outlets) and government organizations (medical authorities) are allowing flexibility in payment options for their services, one being online payment and access to personal records – with this comes the opportunity for others to hack these records.

12. THE HOSPITAL

FIRST AID

The following is a guide to the basic diagnosis of medical conditions.

Hypovolemic Shock (Loss of Blood Volume) – A great many injuries in this list will induce hypovolemic shock, there are a complex set of reactions evolved to compensate for loss of blood pressure. When someone is in shock, blood is diverted from the skin and muscles to the vital organs (and platelet aggregation there is increased). You should note septic shock has essentially the same symptoms (chance of misdiagnosis).

Mild To Moderate Shock (10%-25% of Blood Volume Lost)

The patient will be pale, they will have rapid, shallow breathing, and their heart will be racing. They will sweat, and feel weak. The patient will feel thirsty and their extremities will feel cold. The senses of the patient will be dulled. They might start to feel rising panic from physiological hormonal reactions.

Severe Shock (30%-50% of Blood Volume Lost)

The platelet aggregation in the lungs will lead to respiratory failure. The failure of cellular processes will lead to sequential systems failure (starting with the heart and kidneys). The patient will stop breathing, the heart stops and all the rest of the system will follow in toe within a matter of hours to days.

HEAD INJURIES

Scalp – These wounds tend to bleed a lot (making them a major component of hemorrhaging and shock), they may be purely incident to injuries to the skull.

Skull – The effects of fracturing of the skull is highly dependant upon where the injury occurs – a blow may lead to one of more of the following effects; a mixture of blood and cerebrospinal fluid leaking from the ears, nose or throat, blood may occur in the whites of the eyes, the patient may loose their sense of smell, a loss of vision may occur in one eye, a dilated, fixed pupil, and a worsening in the patient's level of consciousness.

The last symptoms indicate pressure on the brain, caused by swelling of the brain or bleeding into the skull. Swelling of the brain can cause serious damage (or even death in extreme cases), but modern drugs can limit the swelling (and the brain has a remarkable capacity to stop swelling of its own accord). However, if the swelling continues without treatment the hemorrhage will lead to further degradation and death.

The patient may have a headache localized to the injury. They may be lucid for a period after injury, but not quite normal. They will usually feel drowsy, and they may slip into a coma. The patient will generally lose one set of reflexes after another. The patient may gradually lose the use of one of their arms of legs, leading to becoming completely paralyzed on one side. As pressure builds up in the body speech may slur, the breathing will become uneven, and a part of the body may start to shake uncontrollably.

The onset sign of these symptoms maybe hours or days, and the condition may get dramatically worse in mere minutes.

Jaw – A broken jaw will lead to numbness, bleeding from tooth sockets, fractured or missing teeth, the inability to close the jaw properly (the teeth may not meet as usual), pain in moving the jaw, and occasionally bleeding from the ears. A fracture to the jaw might also allow the tongue and other soft tissue to interrupt the flow of air to the lungs, leading to suffocation.

Face – There are any number of bones that can be broken in the face; the face plate, sinuses, cheekbones, the orbits of the eye and the nose. There are a number of different symptoms, but severe facial injury always leads to swelling, resulting in difficulty breathing, inhalation of blood may also take place. This can lead to the patients being unable to breathe within under an hour. There may also be numbness or paralysis in some part of the face. Facial injuries can also lead to hemorrhage and shock.

NECK INJURIES

There are a lot of important functions that pass through the neck, including the spinal cord, larynx, trachea, phrenic nerve, brachial plexus, carotid artery, jugular vein, cranial nerves, esophagus, pharynx, thyroid gland and stellate ganglion. In serious cases, more than one area may be injured.

Spinal Cord – Paralysis, or partial paralysis
Larynx and Trachea – As you breathe through your trachea you will be spitting up blood, a sucking neck wound (see chest wounds), hoarseness, difficulty breathing and a high-pitched noisy respiration (stridor).
Brachial Plexus – Numbness and/or partial paralysis of the arm
Carotid Artery – There will be decreased levels of consciousness, heavy bleeding (which may lead to a compression of the trachea causing difficulty in breathing), and leading to hypovolemic shock.
Jugular Vein – Heavy bleeding leading to hypovolemic shock
Cranial Nerves – An inability to shrug a shoulder or rotate the chin to the opposite shoulder, paralysis of the tongue may occur, hoarseness and difficulty swallowing.
Esophagus and Pharynx – (which connects to your stomach) You may have difficulty swallowing, have bloody saliva, and a sucking neck wound
Stellate Ganglion: Dilated pupils
Thyroid Gland and Phrenic Nerve – There are no short-term effects

The patient might also have damage to the muscles in the neck, which will mean they may have trouble holding up their head.

CHEST (Thoracic) INJURIES

Trauma inflicted upon the chest area can result in damage to the chest walls, lungs, trachea, major bronchi, esophagus, thoracic duct, heart, diaphragm, mediastinal vessels and the spinal cord. In serious damage, a combination of injuries may have occurred.

Sucking Wounds – A person inhales air by moving their diaphragm, which creates a vacuum in the chest region, this in turn pulls air through the mouth down into the lungs. However, if there is a hole in the chest wall, air enters this hole instead (which of course, prevents air getting to the lungs). The patient will obviously feel short of breath, air will visibly being sucked through the hole in the chest wall. If left unchecked the patient could be unconscious in 15 minutes to an hour. It is unlikely however to be fatal on a short time scale.

Tension Pneumothorax – Sometimes the hole in the chest wall lets air in, but won't let it out again (like a one-way valve), alternatively they're maybe a hole in the lung but not in the chest wall (like in the case of a broken rib). Another case is where a patient is treated for a puncture to the chest wall and lung with compression, but air escapes the lung, but not the chest cavity. Under such circumstances the patient's chest will hyperinflate, preventing the patient from breathing. The patient will have rapid, slow breathing. The individual will fall unconscious eventually, and will probably suffocate if left untreated.

Tension Hemothrorax – A similar problem where blood fills up the chest cavity. The patient will probably suffer shock, as well as suffocation. This type of problem usually relates to multiple fracturing of the ribs damaging internal organs. It is often seen with tension pneumothorax (called hemopneumothorax).

Rib Fractures – The major symptom of rib fractures is its hurts when you breathe, which in turn, makes it difficult to exert oneself. The pain is usually in relation to how many ribs you break, however, the breaking of one's sternum is supposed to be especially painful. Beyond the pain, a patient may be lucky and the ribs are not displaced in such a way to cause further injury. The muscles around the bones will generally be enough to hold the chest wall in place.

However, complications can occur like a flail chest, hemothorax, the rib damages the lung, or the ribs displace causing damage to tissue around them.

Flail Chest (Paradoxical Chest Wall Motion) – This is yet another way to suffocate, as the ribs and sternum are broken in such a way that breathing moves air from one part of the lungs to another (than in or out). This will usually result in unconsciousness from low oxygen supplies within 15 minutes to an hour (but not death).

Clavicular (Collar Bone) or Scapular (Shoulder Blade) Fractures – Until a splint is applied there will be pain in moving at all, there is an inability to use the arm effectively. Obviously, it won't be fatal (unless of course a great deal of bleeding also takes place).

Pulmonary Parenchyma (Damage To the Lungs) – Any lacerations to the lungs may result in Pueumothorax, as well as bleeding into the lungs. Contusions (like perpetration from blunt instruments) will cause swelling of interstitial tissues and bleeding into the small airways. In either case, the patient will be coughing up blood and may have trouble breathing. With greater severity, the low oxygen levels may lead to unconsciousness and death.

Heart – Damage to the heart may result in massive blood loss, heart failure, and death in double-quick time. However, less severe damage can result in bleeding into the pericardial sack (tamponade). When the sack fills up with blood, it will put substantial pressure on the heart, making it more difficult to beat (thus lowering blood pressure). The patient will feel initially very tired, leading to increasing stages of shock.

Aorta and Great Vessels (Arteries) – Even with the advances in modern health care, 85% of patients with multiple aortic ruptures will die at the scene, 20% of survivors die within six hours and of the remainder 72% die within a week. Obviously, damage to the heart can result in death in mere minutes. Massive hemothorax and loss of blood pressure are the main symptoms. Blunt instruments initial manifestation of damage is a pain behind the sternum or between one's shoulder blades, difficulty in swallowing, hoarseness and difficulty breathing. If such damage is left unchecked, it may result in hemothorax and increasing levels of shock.

Diaphragm – A chest wound below the nipples is likely to enter the chest, piercing the diaphragm (then entering the abdominal cavity). The diaphragm being the muscle you use to breathe with, means you are likely to have trouble breathing (leading to associated problems like hemothorax, pneumothorax and shock).

ABDOMINAL & PELVIC INJURIES

The main dangers related to abdominal and pelvic trauma is profound hemodynamic instability; resulting from injury to the spleen, pancreas, liver, kidney, or tributaries of the aorta. Most abdominal injuries lead to localized and non-specific pain, nausea and reflex vomiting. Generally, blunt instruments do more damage to the abdomen than penetrating ones.

Intestines – Abdominal and peritonitis may result from injuries to this part of the anatomy. Peritonitis is an inflammation of the tissue that lines the abdominal cavity. After a day or so, the injury will lead to severe abdominal pain and distention, fever, vomiting and thirst – and if left untreated, death may occur in a week or two. It is easily treatable. Injuries occurring to the duodenum can result in more severe symptoms like severe abdominal tenderness in the upper right quadrant and vomiting, within hours. The patient may have hemodynamic instability with time. The evisceration of the intestines isn't automatically fatal, if major hemorrhaging hasn't occurred and the intestines aren't otherwise damage; they may be reconnected. However, poor medical care may lead to sepsis complications.

Spleen or Liver – Abdominal pain in the upper left (spleen) or upper right (liver) quadrant can lead to severe hemorrhaging and resultant in increasing shock and death. The patient needs urgent surgical intervention as the mortality rate for spleen and liver injures left untreated is 100% (almost as high for blunt weapon inflicted injuries).

Sepsis (inflammation or infection) is a major postoperative complication for liver injuries. Splenic ruptures can occur up to 2 weeks after the initial injury (as the initial clot dissolves, the splenic capsule ruptures under pressure from what was initially a small hemorrhage).

Urinary Tract (Bladder & Kidney) – Abdominal pain with be located in the back or flanks, there may be an inability go to the toilet or blood in the urine. Some kidney injuries can result in massive hemorrhaging (where others will not). In the long term, kidney damage may lead to renal failure (which can also be caused by shock and sepsis). Renal failure can last for weeks or months. It is generally fatal 50% of the time.

Stomach Muscles – Damage inflicted upon stomach muscles may make it difficult or impossible to stand up.

Blood Vessels – An injury to the blood vessels in the abdomen may cut off blood supply circulation to the legs (generally resultant in making it difficult to stand for very long). Dependant upon where the injury takes place, a patient's blood vessels may drain into the upper legs, causing extreme swelling.

Pelvis Fracture – A fracture to the pelvic floor will make it impossible to stand, it is also likely that such damage cuts off the flow of blood to the major blood vessels in the legs. Pelvic fractures are commonly associated with massive hemorrhaging.

EXTREMITIES

Generally, minor damage to the arms and legs will make them extremely painful, and make them hard to use on occasion; major damage making them impossible to use. The major blood vessels may be damaged in such incidents, leading to heavy hemorrhaging. Joints can end up dislocated, bones broken, muscles and tendons cut or stressed. Damage to the scapula (shoulder blades) or clavicles will make an arm pretty much useless (until fixed).

Bleeding can generally be stopped by pressure to the wound, if not, you may have to use a constrictive bandage on the major blood vessel pressure points above the elbow or knee. Fractures to major bones can result in massive blood loss (a fractured thigh bone can lead to 1 to 2 litres of blood being lost).

Sepsis – The symptoms for such infections is fever, shock and decreasing mental status, such infections can lead to death if left untreated. It is unquestionably a risk to have operations (or care) in poorly maintain hospitals and clinics.

UNCONSCIOUSNESS

What makes one unconscious is either a direct injury to the brain, lack of blood or oxygen. You lose consciousness in seconds if the blood supply to your brain is lost. Massive hemorrhaging can lead to one's blood pressure dropping fast enough to cause a state of unconsciousness within seconds to minutes. If you lose your oxygen supply, you will fall unconscious in roughly 4 to 30 minutes (depending upon the amount of restriction to the air supply). Poisoning (as in sepsis) can also cause unconsciousness.

BREATHING DIFFICULTIES

Brain damage can occur after only 4 minutes of a person not breathing, the chances of survival are tripled by immediate intervention. Causes for the cessation of breathing include irregular heartbeat, heart attack, injuries or accident, excessive blood loss, drug overdoes and sepsis.

FINAL WORD

This list is designed to give some flavor; not to be used for every injury sustained by the party. If used sparingly, it will engender the desired amount of urgency and heroism. Please note, that there are major blood vessels pretty much all over the body.

PROBLEMS OF SUTURING WOUNDS IN THE FIELD

The basic misconception about gunshot or stab wounds is that they need to be closed up to heal. Unfortunately if it isn't done correctly, it can lead to more problems than not. Suturing is an acquired skill, you risk getting clostridium tentani (tetanus), clostridium perfringens (gas gangrene), staphyloccus, strepococcus and pseudomonas without proper precautions.

Surgeons divide wounds into four areas

- Clean
- Clean Contaminated
- Contaminated
- Dirty/Infected

The classification is determined by the level of bacterial contamination expected within the wound. The first two categories are reserved for patients in hospitals. A clean wound being an area of skin which is cleansed before an operation, and no internal organs are entered – a controlled operation like a hernia is a good example. Clean-contaminated is also in an operation environment, but the internal organs are operated upon under controlled circumstances (often with antibiotic coverage) – like an appendectomy.

Contaminated wounds include open fresh traumatic injuries or surgery with bacterial contamination from an internal organ. Like one slashing your hand with the same knife your have been cleaning fish with. Dirty and infected wounds contain dead tissue, pus, foreign material (like wood, grass), gross contamination (dirt, manure) or are contaminated wounds that haven't received treatment in the first couple of hours after injury.

The following table shows the standard infection rates for each classification

- Clean 1.5 to 3.9%
- Clean Contaminated 3.0 to 4.0%
- Contaminated 8.5%
- Dirty Wounds 28 to 40%

This is where suturing of a dirty wound together becomes a problem, bacteria in a warm, closed space will feed on the bloody injured tissue and multiply rapidly. They can subsequently move on to healthy tissue (causing a wound to turn red and a build up with pus. If drainage doesn't occur promptly, the infection could well spread across the tissue plains causing fasciitis (the so-called flesh eating disease), or spread disease throughout the body, potentially terminally.

With proper cleansing and antibiotics a contaminated wound can be closed without infection, but even surgeons generally leave a wound open initially. This basically allows fluid and bacteria to drain from the wound, whilst the antibiotics kill invading bacteria. After repeated cleansing and antibiotics the wound can generally be closed without complication.

SIX HOURS RULE

The following suggestions for treatment may be of assistance…

Can you get to a qualified medical practitioner within six hours?

YES

a) Stop the bleeding with pressure on the wound
b) Gently clean out any gross debris (like wood, particles, rocks and bullet) but not too vigorously to restart bleeding. It will be painful, but worthwhile. If you have anesthetics use them now. You can inject with a needle to the area, but dripping it onto the wound is also recommended. When it numbs the site of the wound, wet some gauze with the rest and place it in the wound. After a while, cleaning should be less painful.
c) Place a sterile gauze or clean piece of cloth into the opening, if it is near a joint immobilize the limb to stop further bleeding occurring.
d) Transport to hospital, don't take antibiotics unless it will be a long trip (the hospital staff with sample the wound for testing for infection and proscribe the appropriate antibiotic).
e) If there hasn't been a lot of blood loss, and the patient isn't nauseated – you can safely give them pain medication (aspirin thins the blood)

More Than Six Hours

a) Stop bleeding by pressure on the wound
b) Once bleeding has stopped, gently clean out any debris, like wood, particles or rock, but not vigorously to restart bleeding. If you have water, splash over wound: although not sterile it will hopefully lessen the level of contamination. Make use of any anesthetic you have.
c) Place a sterile gauze or clean cloth into the wound, as deep as you can without causing pain. Cover the site with more gauze pads, and wrap the site with a courser bandage to secure. If the wound is near a joint, disable the limb.
d) The wound will seep a lot of fluid and the dressing may need to be changed frequently in the first 48 hours. Continue to cleanse the wound with water/anesthetic. Removing the pack will help to remove the debris that could cause complication.
e) If you have antibiotics give the patient them. Antibiotic ointments could also be useful (place some on the gauze).

If there is extensive blood loss, an open fracture exists, or other serious medical injuries, try to find some form of communication, and summon help to you.

POISONS

The use of poisons in assassination attempts has a long and honored tradition in the world of espionage. It has major advantages over more direct forms of action - as it can be done covertly, and the good assassin can make it look like natural causes. A range of possibilities exist for the administration of the poison including; absorption through the skin, piercing of the skin, ingestion and inhalation. This absorption can be either a one-shot dose, or a number of smaller doses over a period of time.

Thousands of different methods of administration exist, but here are a few classic examples

- Lacing food and drink with poison
- Hidden needles, throwing-darts, sharpened umbrella ends
- Clothing laced with an absorption poison
- Laced gelatin capsules, medicine and injections
- Poisoned Incense, candles and cigarettes
- Deliberately faulty gas fires and ovens

THE USE OF…

To successfully measure out a dose of a poison, the agent will need to have both Chemistry and Forensics knowledge (using the lesser rating). To distill a poison or to synthesis a compound poison, the agent will need access to a laboratory, ingredients and require the same roll. The end result is the potency of the dose (up to poison potency levels listed below). It may take days to achieve such results. Botched rolls may result in the target receiving a lower dose than needed, but may also result in a massive dose being given – possibly resulting in immediate diagnosis (and treatment being sought).

TASTE & SMELL

There are very few poisons that are both tasteless and odorless, making it difficult to administer them without the possibility of detection. Depending upon the circumstances of the poisoning attempt, the GM may seek to roll an Awareness check for the detection of poisons ingested, or for the detection of particularly pungent vapors given off.

VOLUME AND POTENCY

Some poisons are deadly, but require a large dose to be administered – somewhat making them harder to conceal. Two different ratings are given to the following list of poisons. Firstly, Volume of a dose required for it to take effect, and secondly, the Potency of a singular dose. Volume is a rating of the size of the dose (meaning a great deal of liquid, powder or gas has to be used). Potency is the general measure of the effectiveness of the poison.

EFFECTS & DYING

The Potency of a drug determines the roll needed to be made by the victim, the individual's Constitution is the statistic which needs to be rolled – if the roll is under the Potency rating the drug effect takes place, and the difference is deducted from the victim's current wounds (in appropriate cases). If the result equals the Potency rating, the drug's effect *on-set* time is delayed for 10 minutes, but the victim starts feeling disorientated (affecting all rolls by –1). Another roll is required when the 10 minutes elapse. If the victim's roll is over the Potency rating, they suffer no ill-effects from the drug.

The affected victim will need to continue to make rolls each hour or, until a viable treatment is found - or they will continue to loose wound points until they hit *zero* wounds. At this point they will be unable to move from a prone position without help, and they will need immediate hospital care, or they will die (or be consumed completely by the poison's most toxic effect).

One can increase the dosage of the drug, by increasing the Potency rating by 1, however, such activities will generally make it harder to conceal the activity of administration.

LIST OF FAMILIAR POISONS

Antimony: A drug that was widely used in the Victorian era as a sedative, but in large doses can cause death. The drug has the effect of causing abdominal pain if ingested, severe coughing, runny nose and laryngitis if inhaled. It has a slightly bitter taste V 2 P 2

Arsenic Trioxide: This white powder version of arsenic is moderately toxic, but stays within the body for a long time (making it perfect for multiple doses). The drug has the effect of causing severe abdominal pain, rice-water stools, cramps convulsions and fainting if ingested (leading to coma). If it is inhaled it can cause symptoms like coughing , running nose, delirium, extreme prostration – leading to coma. It has no taste. V1 P3

Atropine: This toxin derived from Belladonna (Atropa belladonna) and Jimsonweed (Datura stramonium) can be administered by digestion or by injection into the blood stream. The effects include dry mouth, blurry vision, racing pulse, delirium, seizures and finally, a coma leading to death. The substance has a bitter taste, and the actual source plant is also poisonous. V1 P3

Barbiturates: These synthesized compounds taken from barbituric acid are administered as pain relief, but in large or concentrated doses can lead to depressed heart action, it can also induce a coma – if left untreated, leading to death. It can be ingested or injected. Most barbiturates are addictive over time. They are especially lethal if combined with large doses of alcohol. V2 P2

Botulin Toxins: This waste-product of Clostridium botulinum bacteria, this poison develops in food leading to food poison. It is now widely cultivated and used in the cosmetic surgery industry (Botox). The bacteria cannot survive in oxygen, so it is often hard to use the by-product and cultivate. The effects are vomiting, weakness and diarrhea – if left untreated, it can sometimes lead to death. The poison cannot be detected by taste. V1 P1

Carbon Monoxide: The by-products of vehicle exhausts, this drug inhaled bonds with hemoglobin, blocking oxygen transport to the blood. The initial symptoms include headache, drowsiness and mild disorientation. The effect can also be created by the incomplete combustion of charcoal in a confined space. If left exposed the gas, the victim will finally suffocate. V1 P3

Chlorine: Found as a gas, or in a liquid compound, chlorine is toxic in concentrations as low as 0.005%. Chlorine is also found in a gas configuration; and causes eyes, nose and throat to burn. One will start to cough, wheeze and gag with exposure. If exposure continues, lung capacity can be irrevocably harmed and one can become blinded. V1 P2

Cobra Venom: The milked poison of the cobra venom sacs, is effective injected or ingested. It is highly toxic, but its generally more effective injected into the blood stream. The effect is slow paralysis, leading to heart failure. V1 P5

Chloroform: After inhalation a rush of excitement with sharpened senses, then depression and loss of consciousness leading to paralysis. A burning pain occurs when swallowing, which may lead to vomiting V1 P5

Curare: The drug used effectively by Amazonian hunters in blow-guns for centuries, is a derivative of the vine known as Strychos toxifer. In its distilled form it can cause paralysis of the muscles, leading to heart and respiratory complications. The drug curiously doesn't cause to victim to fall unconscious, and can be used as a crude anesthetic. An antidote exists which is a combination of atropine and neostigmine. V1 P3

Cyanide: Under the group of poisons in the cyanide family include Hydrogen cyanide, which is used as a respiratory poison that dissolves in water (commonly known as prussic acid). Potassium and Sodium cyanide can be used as digestive, blood poison or contact poisons. Death occurs by cardiac arrest. It has the trait of tasting like almonds. V1 P6

Irradiated Thallium: This ingested poison is produced by exposing poisonous metal thallium to intense doses of radiation. Immediate effects include vomiting and nausea, and eventually weakness. The drug eventually kills through the exposure of radiation to the vital organs. The dose required is tasteless. V1 P4

Lacquer: The sap from the lacquer tree can be used as a contact poison, which causes blistering (*1-6 points vitality damage*), or it can be used within a confined space as a respiratory poison burned in a compound. It is easily smelt and causes sneezing and itchiness. V2 P1

Lead: A sweetish metallic taste in mouth leads to a burning sensation in the stomach – abdominal cramps, vertigo, cold sweats and muscular weakness. It would be hard to take enough without knowledge to cause more than short-term discomfort V4 P2

Mercuric Salts: A burning pain in the throat and stomach, throat spasms, leading vomiting and a weak irregular pulse and breathing V2 P5

Nerve Gas: Developed from insecticides during the Second World War and greatly refined since, this family of agents can be absorbed through the skin, eyes and ingested. Effects include headache, vomiting, diarrhea, cramps, violent muscle spasms – leading to paralysis of respiration. Nerve agents cannot be detected by scent, although some still create a visible plume in the air. Exposure effects are measured in minutes, not hours (given the extremely toxic nature of modern variants). There is a dangerous remedy for exposure in *Atropine* – but this is a toxin as well, which may incapacitate the victim and cause harm (*P2*) V1 P4 to 8

Ricin: This poison derived from the Castor Bean (Ricinus communis), widely used for the distillation of specialized refined hydraulic oils is poisonous in its natural form (3-4 beans is enough to kill a human). In a refined state the poison can be used as a blood, digestive or inhaled poison. The onset time for such a poison is generally 12 hours, after which time vomiting and nausea will occur. The poison will eventually lead to kidney and renal failure. V1 P5

Staphylococcal enterotoxin B: The toxin produced by the Staphylococcus aureus bacterium is the common cause for food poisoning. This toxin isn't particularly toxic, but it can incapacitate a target/s and can be easily used in an aerosol form. Symptoms include for inhalation coughing, fever, chills and headaches; those ingesting it can expect nausea, vomiting and diarrhea to follow. A surgical mask and gloves can stave off such effects. It cannot be detected by taste. V1 P2

Strychnine: Produced from the Dog Button Plant (Strychnos nux-vomica) this highly effective drug causes convulsions and contractions within the muscles all at once. The onset time is roughly 15 minutes, and the effect is measured in 5 minute intervals, not hours. Finally, the person will die of paralysis of the respiratory muscles from fatigue. The drug stays active for a couple of hours. Such convulsions are extremely apparent upon the face of a corpse. V1 P6

Tetrodotoxin: The active poison found within the livers of fugu, the puffer fish found in the waters of Japan – and in the skins of and viscera of toadfish, porcupine fish, blue-ring octopus venom and other varieties. It is a digestive poison that causes a tingling sensation and numbness within the fingers, lips, tongue and toes after around 15 minutes. It can also be injected and effects occur within 1 minute. Each successive hour brings the victim closer to total paralysis (including lungs and heart). V1 P8

Dimethyl sulfoxide (DMSO): The solvent derived from wood pulp has the remarkable capacity to carry many other substances through the skin. It can be combined with poisons generally unable to be used as a contact poison.

Binary Poisons: Some poisons (and some non-poisons) have a higher potentiality if mixed in separate harmless amounts – one enhances the other or *potentiates* it. Most nerve gases are mixes of two separate non-lethal gases, but combined they are deadly. Often used as a plot point in murder mysteries, unless the player can make a particularly high roll in either Chemistry or Forensics (6 successes +), the GM shouldn't allow for these in game terms.

A common mix like Barbiturates and the consumption of alcohol, however, is fairly well known and should be allowed.

MEDICAL COUNTERMEASURES

There are limited treatments available for a victim of poisoning. To treat successfully, the person giving First Aid will need to have the appropriate countermeasure/s, and roll over the Potency level of the drug – which will slowly disperse the effects of the poison. The patient's chances are significantly enhanced if they have access to hospital conditions.

These treatments are generally not cumulative in their effects, although intravenous fluids can help in each case – if the treatment lists a particular type of poison + method associated to your case (*-1 off the required target roll down to a base of 1 success required*).

Milk or Vegetable Oil: Helps limit the absorption of a digestive agent. It is especially effective against Antimony and Arsenic.

Immersion: The immersion in water for prolonged periods, helps lower the bodies blood concentration.

Activated Charcoal: The consumption of charcoal can help absorb excess ingested poisons from the system, it is especially effective against antimony, arsenic, tetrodotoxin, atropine, barbiturates and stychnine.

Geophagy: The eating of clay, has a similar effect to charcoal.

Did You Know: Many forms of wildlife eat clay in the Amazon basin to help absorb the toxic effects of nuts and berries within their environment

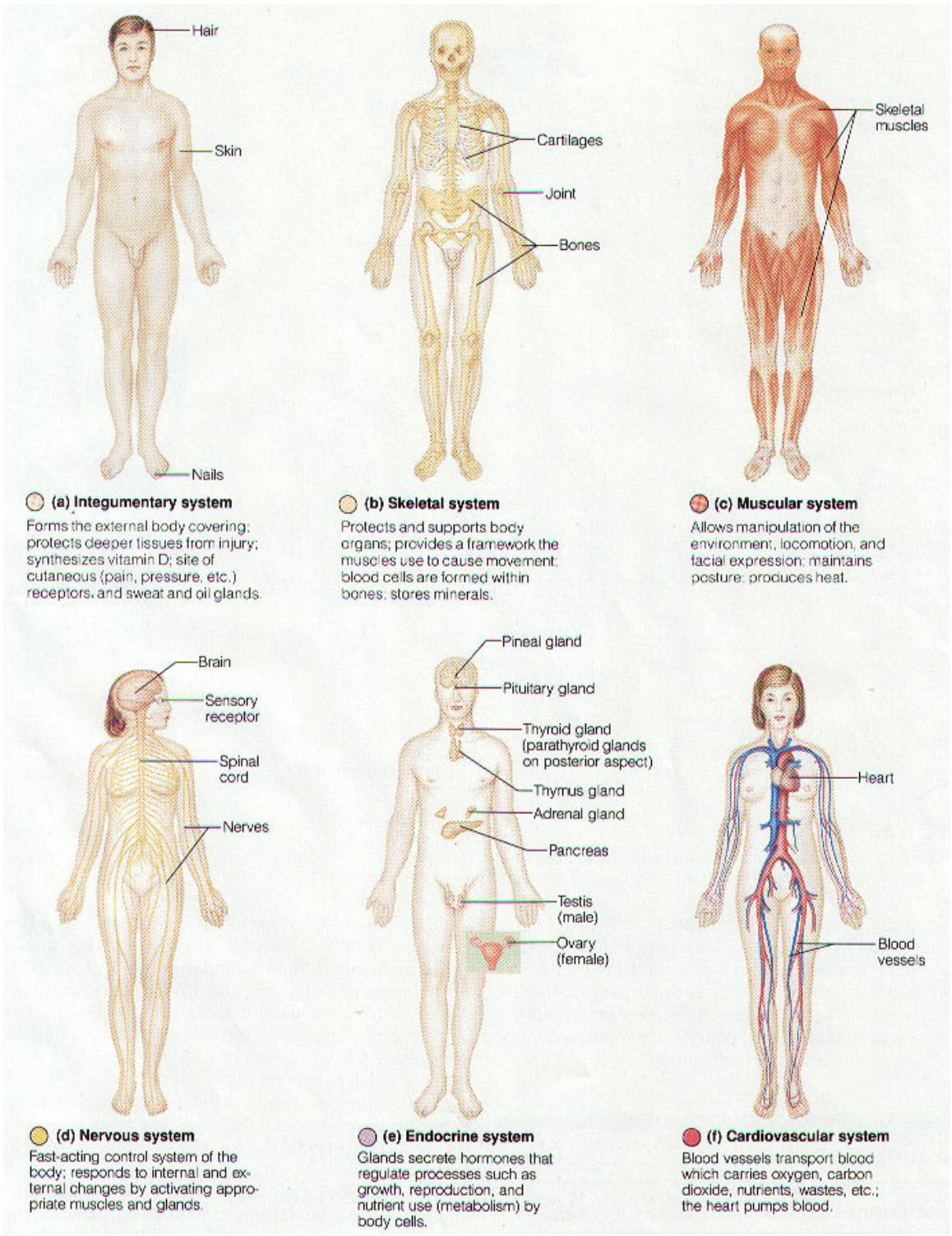
Gastric Lavage: The proverbial stomach pump operation can be performed upon a hospital table, or induced in a patient to throw up in the field, it is effective if performed before an hour has elapsed after ingestion. It is especially effective against antimony, arsenic, atropine, barbiturates and strychnine.

Intravenous Fluids: Help to stabilize a patient who has lost a lot of fluid by sweat, vomit and diarrhea.

Oxygenation: The ingestion of pure oxygen can aid reviving a sufferer of Carbon Monoxide poisoning and those affected by cyanide poisoning (but it must be given almost immediately after ingestion).

Sedatives: The ingestion of sedatives and support care can alleviate the damage convulsions can inflict upon a patient, this is especially effective for atropine and strychnine. The use of sedatives with an overdose of barbiturates is highly likely to prove fatal!

Chelation (Amino-Acid treatment): The injection of such amino-acids helps in the removal of poisons from the blood-stream. It also prevents further damage from antimony and arsenic in the system (a 10-day chelation treatment is generally recommended for patients to stop the chronic affects association with such exposure).



(a) Integumentary system
Forms the external body covering; protects deeper tissues from injury; synthesizes vitamin D; site of cutaneous (pain, pressure, etc.) receptors, and sweat and oil glands.

(b) Skeletal system
Protects and supports body organs; provides a framework the muscles use to cause movement; blood cells are formed within bones; stores minerals.

(c) Muscular system
Allows manipulation of the environment, locomotion, and facial expression; maintains posture; produces heat.

(d) Nervous system
Fast-acting control system of the body; responds to internal and external changes by activating appropriate muscles and glands.

(e) Endocrine system
Glands secrete hormones that regulate processes such as growth, reproduction, and nutrient use (metabolism) by body cells.

(f) Cardiovascular system
Blood vessels transport blood which carries oxygen, carbon dioxide, nutrients, wastes, etc.; the heart pumps blood.

BIO-WEAPONS & CHEMICAL WEAPONS

CHEMICAL AGENTS

RICIN

Castor Oil is widely used as an industrial lubricant and in the brake and hydraulic field, ricin is one of the protein by-products of the extraction process. The ingestion of a mere 2 or 3 castor oil beans is enough to kill an adult, through the bio-chemistry process known as chromatography one can extract the active toxic ingredient.

One gram of processed ricin is enough to potentially kill 36,000 people, such availability of the source material and the relatively easy extraction process by anyone with an undergraduate degree in bio-chemistry, means it is a more likely to be targeted by terrorists than the much vaunted Anthrax.

Symptoms: The initial symptoms include

Ingested: Abdominal pain, vomiting or diarrhoea within a few hours
Inhaled: Fever, coughing, nausea, tightness of chest and difficulty breathing

Within days severe dehydration, decreased blood pressure, internal bleeding, organ failure, respiratory failure and circulatory failure result in death.

Application: The toxin is usually developed into a liquid or crystal form, meaning the application of the poison is usually limited to contaminating food or water supplies; and the smearing of a compound onto surfaces used by the target. It can also be used in tandem with an explosive to cause a limited dispersal to one's intended victims. With advanced access to bio-chemical training, the substance can be converted into a powder – which can carry a far greater distance and cause a greater loss of life.

Cure: There is no known cure or vaccine.

VX

VX is a chemical nerve agent developed by the British in the 1950s. Mainly composed of chorine, the substance in its liquid form is a green slime. It is odourless and adhesive, and almost impossible to remove from a surface it comes into contact with. Britain reportedly traded its research to the Americans in exchange of H-bomb information, and ceased to hold stocks of the agent. America and Russia still hold stock piles of the agent. The major effect on the body is to stop nerve endings communicating with each other.

Symptoms: The substance is extremely potent, causing death within a 1 to 2 hour timeframe of exposure. The major symptoms are paralysis and convulsions. Organ failure will lead quickly to death (*see Ricin for symptoms*).

Application: The agent can be used most effectively in its gaseous or powdered state, as contact with eyes and skin is enough to cause exposure. Used in tandem with an explosive device, such an agent could be as deadly as a nuclear device and leave the area contaminated for a considerable time frame.

Cure: There is no known vaccine, but the application of atropine injected straight into the heart may stop the onset process; however atropine is highly toxic in itself.

BIOLOGICAL AGENTS

CREATING LIQUIDS AGENTS

With a modicum of biological knowledge and equipment, one can quickly take an existing sample of a virus from nature and create a potent agent for bio-terror purposes. With the application of a virus sample and nutrients into vat, and kept at an appropriate temperature, one can quickly grow the viral strain. Once the virus is properly filtrated out through chemical process. The remaining agent can be sprayed over an area (applied to target surfaces or by crop-duster). Potentially, anyone with an appropriate University degree and access to common industrial biological/chemical equipment could set production up in a basement or shed.

CREATING COMPOUND POWDERS

The combination of a chemical compound with an infectious virus greatly enhanced its potentiality, more so, if it can be produced it a powdered state. Preferably the powder should obviate the electrostatic qualities of small molecules (the tendency to clump together). United States and Russian scientists in the 1970s managed to find a way to create such an active compound. The process involves the combining of silica with the virus, and the resultant compound is freeze-dried. The virus is safely held in storage in such a state, and once it is reintroduced to water (eyes, skin, inhaled into lungs), it will quickly multiply and infect the host body. Such a powder requires very little air movement to circulate, and if combined with a denotation device could easily kill as many individuals as a dirty bomb or nuclear device (*U.S tests estimate such a powder in sufficient quantities released could eventually cover ½ million square miles*).

The only potential problem with such a capability is destroying the viral material with the heat of detonation, however there are ways of compartmentalizing the delivery device to ensure such eventualities are slight (*like using bomb droplets, which delay the delivery and effect*).

ANTHRAX Bacillus Athracis

The disease mainly associated with the death of cattle for centuries, in nature rarely affects the human population. However, in 1943 United States scientists working at Fort Detrick, Maryland isolated the infection for biological and military purposes. Although the United States signed off some 26 years later from using its Anthrax stockpiles, the stocks remain in secured bunkers for storage purposes. Anthrax, being an organism existing in nature is relatively easy to isolate and with the application of nutrients in a vat, one can quickly establish a large quantity of the substance. Once the Anthrax has been filtered, the remaining liquid mass is ready for application.

Symptoms: Bacillus Anthracis (inhaled powder) enters the lining of the lungs and the spore shell breaks open and germinates, which quickly multiplies releasing toxins. Symptoms include coughing and eventually leading to flu like symptoms. Mortality is measured in 1 to 30 days (on average, a week)

Cutaneous Anthrax (absorption through skin) & Intestinal Anthrax (eaten) also have the same basic symptoms, but are somewhat less potent.

Application: The substance once filtered becomes a liquid, which can be used to poison food and sprayed upon surfaces. The powered equivalent is far more useful being capable of spreading and potentially infecting more people. This dispersal process can be enhanced by the use of explosives.

Cure: The U.S government has vast stockpiles of vaccines in case of bio-terror. The U.S army has a policy of vaccinating soldiers against such attacks, but doubt is cast over the effectiveness of such vaccines as there are many different strains of Anthrax virus around the world (*being fundamentally a virus*). Most first world countries have somewhat smaller stores of vaccines. The problem with such an infection is diagnosis, with Anthrax having similar symptoms to severe influenza.

The main cure for infection is the application of antibiotics, which need to be administered early before the infection takes a hold (1 to 2 days).

Mortality Rate: 95% (*without quick treatment*)

EBOLA & MARBURG

These group of viruses collectively known as filoviruses cause fever and attack the vascular system causing it to dissolve (*into a mass of blood*). The hemoragic viruses that have caused loss of life in Africa and worry world health organizations are prime targets for isolation and use in bio-terror.

Symptoms: At onset flu like symptoms occur, eventually resulting in fever. After a number of days the patient will become weak and become bedridden, with blood flowing out from their mouth, rectum and nose. Death results in 3 to 12 days.

Application: Because of the highly contagious nature of the virus, it is seen as difficult to produce and use effectively. However, if a terrorist is committed to giving one's life to the cause, the individual could be voluntarily infected before their flight to a target destination; or a slow release of liquid into ventilation shafts of highly accessed public areas such as train stations could be orchestrated. It is possible that a powdered form could be produced, but excellent facilities and knowledge would have to be procured.

Cure: There is no known cure for the virus, making it less likely that a terrorist would use such a vehicle for the loss of life (*as the infection could potentially leave the target zone to other countries and areas*).

Mortality Rate: 70%

SMALLPOX

The Variola virus that was wiped from the face of the Earth by the World Health Organization in the 1970s is still retained in stores in the U.S and Russia. The virus, which invades the body's blood cells and destroys them to reproduce itself has been retained under the behest of keeping samples incase *further outbreaks should occur*. However, it is just as likely it has been retained as a potent threat if their civilizations should come under threat in the future. As a bio-weapon smallpox is seen as limited in application as infection rates are low, mortality limited and a vaccine is readily synthesized.

Symptoms: Early symptoms include a rash and high fever, within 2 weeks flu like symptoms occur and the distinctive small white pustules occur on the skin. Death occurs within 7 to 17 days.

Application: It is hard to imagine a terrorist organization resorting to using such a virus, however, it is assumed if one could obtain such a contagion, one might be able to synthesis a virus of greater virulence and infection rates. It could theoretically be produced in both a liquid and powder form.

Cure: There are a number of vaccines available for dealing with smallpox. Antibiotics have a limited effect upon early diagnosis.

Mortality Rate: 30%

PLAGUE

Yersinia Pestis is the virus that ravaged across Europe for centuries (wiping out a 1/3rd of the population in the 14th Century). Plague can be found in 3 different forms: Bubonic Plague (infection of the lymph glands), Septicemia Plague (infection of the blood) and Pneumonic Plague (infection of the lungs). Pneumonic plague is the form that can be spread between individuals. Plague is a bacterial disease of rodents, which can be spread to humans and other animals by infected fleas.

Symptoms: Once the infection has occurred the bacteria will generally move to the lymph glands causing a swelling to occur (the painful lumps called buboes). Other symptoms include high fever, headaches, chills and extreme lethargy. If left untreated severe blood infection will occur. Symptoms generally appear 2 to 6 days after exposure. Those with pneumonic plague will also experience difficulty breathing, coughing and bloody sputum.

Application: Once infection occurs the disease can be spread by pneumonic symptoms (coughing and exhalation of bloody sputum), such diseases can spread quickly, but in a rather indiscriminant fashion – making it an unlikely target for synthesis as a biological agent for all but apocalyptic cults.

Cure: If diagnosis occurs in time, the disease is treatable with antibiotics (usually streptomycin)

Morality Rate: 30% left untreated

13. TRAINING FACILITIES

INTELLIGENCE CYCLE

PLANNING & DIRECTION

Any intelligence operation is inherently political, from Sir Francis Walsingham spying to stabilize the reign of Elizabeth I in the 16th Century to the excesses of today's use of the *Al-Qa'ida* threat of *Jihad* being used to push American interests in the Middle East. Despite the abundance of mythology associated with the Cold War, the *Great Game* was essentially about asserting one political ideology over another.

The *terrorist* of today, could be the next Nelson Mandela.

It is important to realize that Intelligence gathering is a political act. The institutions we may hold to be benign servants of the public good, are fundamentally dedicated to preserving one particular way of life. For example a University seeks to maintain the central core of *common sense* beliefs, investment banks seek to maintain their domination over the wealth creation process (mainly for those few already with the majority of existing money supplies), and the Police and Law functionaries of the State seek to maintain the *order* by repressing and outlawing various forms of subversion.

Hopefully, the previous didactic passage goes some way to show that alternative point of views are marginalized within societies – it's not always a conspiracy, societies need to impose a shared set of values. But what does shows is, all events are open to interpretation; the *freedom fighter* often has a different perspective on events we come to classify as pure barbarism.

Any intelligence agencies charter is planned according to the current governments values, needs, prior cover-ups, past institutional problems, or the desire to reassure the public of an agencies competence. A case in point is the number of Western intelligence agencies after the fall of the Berlin Wall and the end of the Cold War – they sought to redefine potential threats to maintain their funding levels (like the CIA changing from Soviet to Islamic threats and the *War on Drugs* in South America). The CIA recently has even reconfigured their basic operational focus from SIGINT back to the ever reliable HUMINT.

Although Planning and Direction don't inherently come into planning operations, only a foolish agent would ignore implications of working against the interests of their government and agency.

COLLECTION

Once an agencies agenda has been set, the act of collecting data can take place. After the atrocities sponsored by Al-Qa'ida on September 11, 2001: it was inevitable that the U.S intelligence community would focus their activities on gathering information on the terror organization. From the training of agents in Arabic culture and language, recruiting foreign agents to gather information, targeting signal transmissions from within Middle-Eastern states. It is a well-known trait that if you concentrate a police force in a certain neighborhood, you get a sharp rise in lawbreaking. It has little to do with the criminals, and everything to do with police saturation. The same phenomena happens in intelligence gathering, it is good for funding purposes to occasionally redefine your list of targeted groups – knowing that it will generate its own impetus.

Before any type of operation (whether it be intelligence or military in nature) the basic procedure of gaining the requisite information to base judgements upon is often the key to success, whether this be from observation via satellite or close target reconnaissance.

PROCESSING & ANALYSIS

Once information has been gathered from the field it needs to be sorted, graded, scrutinized, matched, decrypted and analyzed. The real myth of intelligence operations is that the hard job is *collecting* the information. Finding the connections between apparently random bits of information and second-guessing the mind of the foreign power *is* intelligence. For all the signals the British picked up in War World II, without cracking the Enigma (decryption device) code by the use of the computer known as Colossus, the war might very well have turned out differently.

The major portion of intelligence professionals are employed doing time consuming jobs like decrypting information and developing specialist knowledge areas to break every piece of the intelligence jigsaw.

Once the information has been assembled, analysis can take place; often this becomes the basis for subsequent operations to gain further information, or to remedy the situation.

DISSEMINATION & DISTRIBUTION

Once the information has been put into some form and operational requirements have been met, the information is used in some tangible way. The art of counter-intelligence is disinformation; the Cold War's Great Game derived its title from the necessity to separate fact from fiction. Acquiring good intelligence from a foreign power isn't just a reward in itself, it can be turned back upon them. Through the activities of the Atomic Ring of Spies in the 1950s, USSR was able to gather intelligence on America's nuclear capability – eventually replicating the program, and advancing their influence and forces throughout Eastern Europe.

All external Intelligence agencies have divisions devoted to creating and disseminating propaganda, a standard ploy of the CIA is to drop leaflets by plane in hostile foreign countries to civilians to overthrow their government.

DEAD LETTER DROPS

A basic skill in any intelligence officer's tradecraft skill set is the use of dead letter drops. An officer will frequently have to get in contact with their agents. The proper use of dead letter drops will obviate the need for face to face contact – that runs the risk of exposing their affiliations. A prearranged neutral location is used, whether this be in an up-market fitness club, parkland, urban wasteland or forest. The key ingredient here is to either be alone in the environment, or in an environment where their subsequent activities won't raise too much attention. The basic dead letter drop requires a signal and a location for the dead letter. A marker is used by an individual to show that a drop has been made, whether this be a rock on a wall, a crayon mark on a building or any other activity that can be readily deciphered. The other part of the equation is the location where the note, document, cash etc can be left undisturbed. This place is often in a public space, it might be a canister hidden under a rock, a plastic bag submerged into a public toilet or any other location it can be successfully retrieved from. Successful spies have used putting notes into tennis balls on a tennis court, or throwing Coke cans out into scrub lands in rural settings; the form of the dead letter drop is truly up to the imagination of the intelligence officer.

Running Agents – Any handler or intelligence officer needs to be able to select and target a potential agent with due care and diligence. It often seems contrary to accepted wisdom, that the person willing to offer up the most information, is generally the last agent you should have working for you. Their over-eagerness may be a sign of them being a double agent, or it may be a sign the individual is seeking attention (they may be making up the information to meet your overeager expectations).

The 4 classic motivations for people to become spies can be summed up in the anagram…

MICE

MONEY If you do enough digging, you will generally find out that at any one time, most individual's want either; money to pay the bills, the latest technological wonder, or just a nice holiday. Most agencies can offer such pin money for information, generally increasing the payout to match the greater degrees of risk needed. Once this pattern is established, and the agent is addicted to the extra income, the agency virtually holds all the cards - because they can expose the agent at any time if they refuse to co-operate.

IDEOLOGY Everyone subscribes to some level of political, religious or social ideology that can be used to manipulate him or her. Whether they are intent upon purifying the Middle East of capitalist tyranny, or simply interested in local land developments - in the greater context even minor individuals may be useful for getting at people of greater and more dangerous associations. Another avenue of approach is to find a formerly committed target whom may be feeling disenfranchised and bitter at changes to their cause, they may be persuaded to solicit some kind of orchestrated act of revenge - on behalf of the host agency. It is often the case in extremist causes that the most committed participant is the first to fall out with the causes' leaders.

COMPROMISE A lot of intelligence time is devoted to finding the necessary hooks within a target's personality to allow an agency to manipulate them or to look for patterns that may weaken their stance within their fraternity. Of course, if you cannot find any, it may become necessary to *generate* some. From sexual entrapment operations, to plying the target with drinks and making up stories, to even actively generating false criminal records to promote their compliance. The classic strategy is to allege their visa details are out of order, and demand them to perform certain steps to receive the agencies help in clearing up the matter. Ultimately, the agency may seek to contrive a situation whereby greater and greater consequences are built-up every time they deal with the agent – much like the Mafia demand continued *respect*.

EGO Intellectual flattery is a valuable tool in establishing an agent, it is not enough that they acquire the necessary classified material; they desire to be regarded as agents of intelligence and wit, demanding the respect of the host agency. The famous British Cambridge Spies of the 1950s original motivation is thought to lie in the danger and excitement of spying - consequence of an agent's actions are not clearly established until the agent has crossed the line between thought and action.

Did You Know: A classic exercise used by the British Secret Service (MI6) in training is to send a trainee officer into a nearby pub and give them one hour to find out the following information about a stranger – Forename, Surname, Age, Date Of Birth, Job and Address

RADIO TERMINOLOGY EXAMPLE

The following series of surveillance terms are taken from the operations of the former British military intelligence unit *14th Company*…

Zero – The net callsign of the control station in charge of the operation

Alpha, Bravo, Charlie – Reserved radio designations of surveillance targets; Alpha 1 being the target's residence, Bravo 1 being the target, Charlie 1 being the vehicle they drive.

Bingoed – A British surveillance term for being discovered by the target

Click/Double Click: In situations where the operator might be compromised by maintaining verbal communications, they * click * once to confirm 'no', or **double click** for 'yes'.

Complete – As in the controller or target is returning to his car, as in 'Bravo 1 is complete in Charlie 1'

Going Complete – A British surveillance term that generally means the individual has lost sight of the target (i.e. gone inside a shop)

Contact – Visual Contact

Delta through to Zulu – Reserved for operators (surveillance team), who usually keep their same callsigns throughout all operations.

Eyeball – To have visuals on someone, having eyeball on the target.

Foxtrot – Travelling on foot, as in 'Bravo 1 is foxtrot towards Charlie 1'.

To Have – To have visual contact, as in 'Zulu has Charlie 1 intending left'.

Intending – The signal for the likely destination of target, as in 'Bravo 2 intending left'.

Mobile – Travelling in vehicle, as in 'Bravo 1 is foxtrot from Alpha 1 to Charlie 1 and mobile'.

Off – No longer in visual contact with the target, as in 'Charlie 1 is towards Alpha 1 and I'm off'.

Two up, Three up – the number of people in a vehicle

Possible – to qualify an area of doubt in information as reported. As in 'Zulu has possible Charlie 1 mobile'. If it is then confirmed to be a wrong assumption, 'Zulu, that's a negative'.

Spot & Color Codes – Operational centers are usually color coded and split into segments along the lines of Red Two Four, Red Two Five, in basic quadrants. This is to not give away the operational areas discussed to eavesdroppers. These are usually fixed, and officers generally learn them in the field before they officially start being involved in operations. Furthermore, each street in an operational area might be designated a color code as per an individual mission. Thus, 'Charlie 1 is mobile from Purple towards Brown'.

To Stake Out – To box a target into an area by controlling all exit routes. In Northern Ireland R.U.C officers might set up vehicle inspection points.

Standby, Standby – An expression used to warn all the surveillance team of a significant movement of a target, usually used sparingly as it generally means the need to scramble the operational team out of the presumed operational zone.

Shorts & Longs - A term to denote the carrying of pistols (shorts) or rifles/shotguns (longs)

ALPHA	NOVEMBER
BRAVO	OSCAR
CHARLIE	PAPA
DELTA	QUEBEC
ECHO	ROMEO
FOXTROT	SIERRA
GOLF	TANGO
HOTEL	UNIFORM
INDIA	VICTOR
JULIET	WHISKY
KILO	X-RAY
LIMA	YANKEE
MIKE	ZULU

A STUDY OF ASSASSINATION

This summary is of a CIA guide to Assassination that was released during the 1950s…

Definition: The term assassination is said to derive from Hashish, a drug similar to marijuana used by *Hasan-Dan-Sabah* to motivate his followers, who were assigned to carry out political and other murders.

The basic definition of Assassination is the planned killing of a person who is not under legal jurisdiction of the killer, who is not physically in the hands of the killer, who has been selected for death by a resistance organization, and whose death is beneficial to its cause.

Employment: The U.S government, like a lot of similar governments around the world, do not condone assassinations. The reticence is partly due to the need to commit such acts to paper, and partly due to murder not being seen as morally justifiable. However, if the career of the foreign national is seen as clear and present danger to U.S policy, it has been known for intimations to be made that certain individuals would *not be missed.* This anomaly of statecraft has undoubtedly been practiced for many millennia, however, exposure of the practice to the general public always raises a lot of moral outrage and discussion.

CLASSIFICATIONS

Simple: An unaware subject
Chase: Victim is aware of the threat, but unguarded
Guarded: The victim is guarded

Lost: An operation where the assassin will be killed
Safe: An operation where the assassin is presumed to return safely home

Secret: An operation where the victim is presumed to have died naturally
Open: An operation where no precautions to conceal the assassination have taken place
Terroristic: An operation where publicity for a cause is part of the remit

As such, the assassination of Julius Caesar was safe, simple and terroristic.

The Assassin: The assassin should be able to perform their operations clandestine and be ever resourceful. Generally, an assassin should be secular to the organization seeking to affect the death. Instruction should ideally be given only to that one person, contact should otherwise be sparse. In lost assassinations, generally the individual will be a fanatic willing to sacrifice their own life for the cause. He must not know other people in the organization, and careful man-handling is required for someone who maybe unstable psychologically.

Planning: Effective planning should be undertaken to reveal gaps in information, laxity of security and special equipment needs. No details should even be written down.

Techniques: The essential point of assassinations is that death should be effected. Death should be absolutely certain. One should always attempt to come up with a simple plan; a plan with too many variables is a poor plan. The following different methods should be considered…

Manual – It is extremely difficult for an untrained person to kill with their bare hands, locating a simple tool laying about (like a lamp stand or kitchen knife) will increase the odds. A length of rope, belt or wire is good for agile, strong people. It maybe preferable to use whatever is available at hand, than to carry in specialist weapons (for the fear of being searched), however, in safe operations careful consideration should be given to the disposal of the improvised weapon.

Accidents – Such accidents are preferable in most cases because it generally raises far less comment. A fall from 25 meters or more onto a hard surface should suffice. Falling into water is not recommended because of the chance of failure to kill. Although, a fall into fast flowing waters by someone who can't swim, may.

Automobiles, trains and subway cars require far too much precision and allow for a chance to be seen. Tampered vehicles have a very low rate of reliability and may be discovered. Drugging a victim and then pushing the vehicle over a cliff et al, may prove effective. Alcohol may be used for heavy drinkers.

Arson may be used on drugged people, but a lack of reliability in a building burning with enough combustion should be considered.

Drugs: The use of drugs can be highly effective (unless your cause is terroristic in nature). An overdose of morphine to a patient (by a *doctor*) can cause death without disturbance, and detection. If the target drinks heavily, a barbiturate or morphine can be used at the passing out stage. Specific poisons like arsenic and strychine can be used, but may be found in one's possession (incriminating oneself).

Edged Weapons: May be used, but to be successfully employed one needs to puncture the heart in the body cavity (not as easy as it sounds). Abdominal wounds *used* to be mortal, modern medical treatment can successfully treat such wounds. Absolute certainty can be obtained by severing the spinal cord in the cervical region (which can be performed with a light blow). One can also severe the jugular and carotid blood vessels on both sides of the windpipe. Finally, this can be achieved with more ease if the subject has been previously drugged.

Blunt Weapons: As with Edged Weapons, Blunt Weapons require some knowledge of the anatomical structure of the body. Blunt weapons are preferred because they are universally available; think of a hammer or a baseball bat. Blows should be directed to the temple, the area just below and behind the ear, or any portion of the lower, rear portion of the skull. The lower frontal portion of the head (from eyes to throat) can withstand enormous blows without fatal consequences.

Firearms: Are often used in assassinations, and rather ineffectually. You need to know the technical limitations of the weapon before use. You should start by halving the effective ranges you have in mind for the weapon (due to the accuracy and killing power). Firearms are also incriminating if discovered, and they do require some skill to use effectively.

A good hunting rifle can effectively be used at up to a distance of 250 meters (100 meters being optimal). You should use a rifle made with a bolt or falling action, the use of hunting long-range cartridges (.270 Winchester) should be used instead of military issue, which have fully jacketed ammunition (which has less stopping power). You should use a telescopic sight incase of dim light. With the use of such a caliber weapon, death should be certain.

The machine gun can be used upon individuals in a 5 second burst, if the burst pattern is no larger than a man, it should kill anyone, even with a full jacketed ammunition. This can be accomplished at a range of no more than 150 meters. A good quality machine gun can do it at around 800 meters. Care must be taken to make sure the first bullet hits the mark, as training tends to specify targeting effectively takes place *after* the first bullets have hit their mark – you may not have time to wait.

The sub-machine gun is somewhat useful in assassination. This is a short-range weapon; one should use it within 45 meters or less. You should endeavor to spray 5 rounds into the subject's chest – as the relatively smaller .45 caliber rounds used in pistols is much less powerful. SMGs are of particular use within indoor areas, and two gunners can spray a medium size room within 15 seconds.

The large bore shotgun is most effective as a killing instrument as long as the range is less than 10 meters. It should normally be used on a single target, and obviously it isn't an instrument for sustained firepower. The barrel may be sawn off for ease of concealment, which doesn't adversely effect the operation, .00 buckshot is considered the best ammunition, although even buckshot at the right distance will cause death. The assassin should aim at the solar plexus for maximum stopping power.

The pistol is quite inefficient as a weapon of assassination. The pistol should be powerful and fired at just beyond a person's reach. Larger caliber weapons are preferred and the subject should be hit with at least 3 shots for complete reliability.

Silent Firearms: The use of silencers is problematic, being sniper rifles don't really need such silencing capabilities (being far from the target) and individual's using pistols and shotguns (are too close for it too make much difference). No silencer can stop the shock-wave caused by barreled weapons (rifles), so a great degree of sound is generated. Even silenced pistols create noise, just not a great, distinctive noise.

Explosives: Are used a lot in terroristic or open assassinations, not always effectively. The major problem being the accuracy and precision needed to set them off at the right time, but on the plus side, the assassin doesn't generally have to be close to the target. Plus, indiscriminant killing of civilians from bombs may hurt a terror organization, rather than help.

Bombs and grenades should never be thrown; it is an unreliable method.

Five kilos of explosive should be regarded as a minimum used, other material which is hard (like metal or rock) should also be packed in for maximum damage (walnut sized). If metal plates are used, make sure not to make the casing thicker than 1" thick. Homemade bombs should be avoided. Anti-personnel mines are excellent, as well as 100 mm or larger mortar shells or howitzer shells. The device should be placed within 2 meters of the target.

A large shaped charge with nuts and bolts and iron fragments will fire up to 45 meters away, and the device used should be test fired before the operation to determine any potential weaknesses.

An electric triggering device should be used, or the use of a mobile phone duly rigged to detonate upon calling the number is excellent.

BODYGUARD TECHNIQUES

The leap from bouncer to professional bodyguard requires a great deal of study and competence; rarely will international agencies take on someone without extensive specialist training and experience. There is a lot of work for bodyguards protecting diplomats, celebrities, business executives organized crime leaders and royalty, some paying handsome sums for peace of mind.

There are a number of international agencies offering comprehensive training for bodyguards, however, there are also a number of charlatans – a professional course will offer training in the following…

- Defensive Driving
- Escort Drills
- Firearms
- Close Quarter Battle
- Communications
- Electronic Counter-Surveillance
- Bombs Disposal (IEDs)
- Paramedic Training
- Risk Assessment, Planning and Preparation

CLOSE PROTECTION TEAM

One individual will be in charge of all aspects of the operation, called the *Body Guarding Commander* (BGC) – who will stay with the *Principle* (the individual primarily being protected) at all times. This individual will decide how many other bodyguards (BG) are needed in the *Close Protection Team* (CPT)– 5 member teams are enough to protect the Principle from medium levels of threat. The commander will generally recruit trusted bodyguards they know and have worked effectively with before, although some jobs they will be required to direct existing security personnel, and give reports as to the staff level of competence. Judging how the team will react under pressure situations is part of the job of the commander; ill discipline may very well compromise well-laid plans.

EQUIPMENT

The following items are generally on the top of any commander's wish list…

Sunglasses - Are important to disguise the observation of suspicious activities without being detected
Sig Saur 9mm Pistol x2 spare clips – A reliable pistol with a relatively low recoil (making it easy to use and accurate), usually carried on the hip
Heckler & Koch MMMPK Sub Machine Gun x2 spare clips – It's relatively small size means it is easily wielded in vehicles and concealed under arms
Retractable Baton – Being retractable means it can be concealed effectively
Encrypted Radio, Earpiece and Hand Presser: For covert communications
Walther P99: Is sometimes carried as a backup weapon in an ankle holster, making it easier to reach when one has dived on the Principle

The commander will generally have a Sig Saur 9mm pistol, retractable baton and Radio, as their main function isn't to return fire, but to direct and protect the Principle.

Other equipment usually in the vehicle…

Heckler & Koch 33 x2 35 round magazines, retractable stock and red-dot laser sight – With a greater stopping power and range, it is best for protracted fire-fights
S10 Respirators – Used in gas attacks
Torches: Various torches for night time activities
Heavy Body Armor – This type of armor will stop a hi-powered rifle, however it is big, heavy and obvious, which may be at odds with the strategic plan
Lightweight Body Armor – This type of armor will generally stop a thrust from a knife or 9mm bullet, which will generally be of more use to bodyguards
Emergency Medical Equipment: May or may not be included
Umbrella – To protect the Principle from rain
Blanket – For covering up weapons in the boot, and to comfort the injured

MEETING THE PRINCIPLE

The BGC will need to hold in-depth discussions with the Principle before starting an assignment. The discussion will involve seeking out the needs of the principle (whether they are going from point A to point B, will they stop to meet civilians in the street, any unique needs of the principal etc). The principle may be concerned about the wrong image of being circled by security; some compromise may need to be discussed.

After discussions with the client the BGC will try to obtain a situation report (sit-rep) from the local security service from the place they will be operating in (including information about local prominent figures, terrorist organizations within the area and direct threats against the principal). Often such information needs to be collected through less formal channels.

ROUTE RECCE

The BGC will then seek to do a *recce* of the area, either in person (if no risk is entailed) or get someone else to do it, the route will be filmed and analysis will take place looking for *key danger points* (these points will generally be given a number, so later the BGC can talk the team through these dangerous areas).

VENUE RECCE

The same activities will take place at the venues the principal will be visiting. Each side of the building will generally be designated a color (white normally the front), and all entrances and emergency exits will be given a number (designed to aid quick communication in case of complications).

DISCUSSING SCHEDULE WITH PRINCIPLE

Once a plan has been developed, a meeting is set up with the principle to work through the schedule. The principle needs to be informed of the process and given a schedule to follow; it may be altered by the dictates of the principle – usually they will take on board the advice of the BGC once the dangers are explained, but last minute changes to the schedule need to be discussed and planned for. The principle is educated to certain safety requirements and alerted to any contingency plans in case of incident.

BODY GUARD METHODS

There are three main tactical decisions to be made…

Military Overt, Low Key Overt or Covert ?

Is it necessary for the operation to be low key operationally, where weapons are hidden and the principle is still visible, or is it necessary to show force of arms (military overt) and keep the principle somewhat hidden. Or is it better to be covert (where even the principle doesn't know they're being protected, and therefore, neither does anyone else). Each have their own strengths and weaknesses. It may be necessary to show some force in a war-zone, where it might be better to be low-key at other times to flush out surveillance and potential assassination plots.

FORMATIONS

There are three main formations used by Close Protection Teams…

Open Box Formations – the box formation where the BGC stands beside the principle, and is flanked by four BG, it provides only minimal protection as the BG are not directly around the principle
Close Box Formation – the BGs stand arm to arm with the principle and BGC, it provides good protection from firearms and hand-held weapons, but all may be killed by a grenade attack
Arrowhead Formation – the V-shape provides the most flexibility and is usually used by most agencies. Two flank men protect left and right, and flank. The BGC stands to the right of the principle and another BG stands not far away to the BGC right. This allows the BGC to move effectively around to meet threats knowing that the BG beside him will cover.

DRIVING

It is essential that all bodyguards are trained in advanced driving techniques (both offensive and defensive), the objective being to keep the convoy moving; getting away from danger as fast as possible. It is ideal if the principle is moved in an armored vehicle, although one can improvise by having two BGs placed in the driver and passenger seats (giving some protection from the front of the vehicle). Most cars used will have the airbags and emergency fuel cut-off devices disabled in case of a crash (the vehicle will need to move even if involved in a crash scenario). Sometimes remote control cameras are fitted to these cars, for remote viewing capabilities.

DANGER ZONES

In the Route Recce process, the following hazards (Danger Zones) should be noted and cataloged with numbers for operational use…

Roundabouts – Are particularly dangerous due to the opportunity for the ramming of the car from vehicles coming the other way around (the wrong way around the roundabout). Besides, it is easy to box in a target vehicle in between hostile vehicles (the vehicle can even be rammed in the side from vehicles coming from left and right).

Bridges – Are an obvious place for terrorists to hide and drop explosives from (or launch handheld rockets).

Hedges/Woodland – Can provide adequate cover for concealment

Choke Points – Double bends in roads, sharp turns, areas where the road is narrow, pedestrian crossings should all be accounted for.

Everyday Scenes – Workmen slowing traffic with signs, cars being checked at the side of the road, road accidents – typical everyday occurrences, however, they may be manufactured to slow things down; one must always be aware of the potential for an accident. A lead vehicle will hopefully make the BFC aware of such incidents ahead.

EMBUSSING

A standard procedure used to evacuate the Principle from a hostile scene, requiring a 5 man team and 3 cars. If the principle is under attack, s/he is bundled into the middle vehicle (Charlie 2) by the BGC. BG 1 covers the BGC and principle into Charlie 2, then provides cover for the rear of the vehicle. BG2 will cover the front of Charlie 2. BG 3 moves to Charlie 1 (front car) and covers the *bug-out* (exit of Charlie 2 will leave from). BG 4 covers the rear of the convoy. Once Charlie 2 is away it will head to a prearranged *emergency rendezvous* (ERV). Then BG 1 & 2 enter Charlie 1 and BG 3 & 4 enter Charlie 3 (back car) and hopefully join Charlie 2 at the ERV.

DEFENSIVE DRIVING PROCEDURES

The most important aspect of the convoy is to keep it moving, if there is an immediate threat to the convoy the lead car with use offensive driving procedures (like ramming it).

Turning Right (Left) – When turning across traffic Charlie 1 usually angles across the road and allows Charlie 2 to pass, Charlie 3 will then overtake to take over lead duties. This stops Charlie 2 from being exposed (even if momentarily, to traffic coming the other way).

Crossing Traffic at T Junction – Charlie 3 will overtake both vehicles and block oncoming traffic whilst Charlie 1 and Charlie 2 progress (and Charlie 3 resumes the rear position).

Overtaking Vehicles – Charlie 3 (at the rear) pulls out to prevent overtaking vehicle from progressing up the convoy.

AMBUSH SCENARIOS

Frontal Attack

If the convoy is attacked from the front, Charlie 1 stops and the BGs gets out and lay down heavy fire (hopefully with the H&K 33), whilst the BGC either drives Charlie 2 away to safety, or even bundles the principle into Charlie 3 and reverses back the other direction.

Side Attack

Hopefully, it is just one side the Charlie 2 is blocked in, which makes it easy to ease the car off in the other direction whilst Charlie 1 and Charlie 2 bodyguards provide cover fire. If the convoy is blocked from both sides, it may be necessary to put the principle in heavy armor and move him/her to the vehicle at the front or the back to escape. It may seem easier to keep the principle down until the firefight is won, but further hostile forces may also be on their way.

Ambushed On Foot

Generally the process is to use a point guard to deal with the hostile force, even using another BG to help lay down cover fire, whilst the principle and BGC back away to cover, with cover from the other two BGs behind – then the BGC can call for a vehicle to vacate the scene.

TERRORIST OBJECTIVES

The activities of terrorist groups is not random, thoughtless violence. Terrorist activities are generally meticulously planned, as part of an orchestrated campaign to achieve specific objectives. In much the same way as politicians use *spin doctors* to gain preferential media treatment and air time – a terrorist bomb is planned to achieve maximum media attention.

Bruce Hoffman in his book 'Inside Terrorism' discusses how a typical terrorist campaign moves through phases to achieve wider recognition.

1. Attention – They grab media attention through a series of dramatic, violent acts
2. Acknowledgement – They may gain acknowledgement (even sympathy and support) for their cause
3. Recognition – The group is recognized as spokesmen of the people they claim to represent
4. Authority – They gain some legitimacy for their movement, and influence changes in government policy and/or society
5. Governance – The terrorist group consolidate with some investiture of civic power, effectively becoming the new Government hierarchy/establishment

One can compare the image of Nelson Mandela as a terrorist in the 1970s to becoming the President of South Africa in the mid 1990s. Although his personal journey from terrorist to pacifist is emblematic of the radical change in the social conscience of the nation, it is a rare exception to the general ethos of the ANC movement throughout its campaign. Some would say, without the innumerable car bombs in packed city streets the *redemption* of Nelson Mandela would not have been such a powerful narrative for constituting social change.

TERRORIST TACTICS

At the start of proceedings, it is very much in the terrorists' interests to stage the most sensational acts of violence. The bigger the bomb, the more victims kill or injured – the greater the media impact. It is generally best if the act has never been perpetuated before, as many a would be plane hijacker found out in the 1970s after a Palestinian liberation group did a series of hijackings and created a firestorm of media attention. Unfortunately, human nature being what it is, we are fascinated by the loss of life in a unique way (like the Twin Towers in New York) – despite the horrible loss of life, the incident *was* audacious and metaphorically charged.

The terrorist always has the upper hand in dealing with security forces. The terrorist sets the agenda, whilst security forces must constantly be alert and engaged. The terrorist group only has to be lucky once; the security force has to be lucky all the time.

Intelligence is the most power weapon available to security forces. Physical security measures like checkpoints, patrols, internment may be of use for a limited time; but may be counter-productive in building up support for the group's claims of suppression.

As a terrorist movement gains respectability and influence (even if begrudgingly so), the group may renounce violence somewhere between steps 3 and 5. To continue to do so would be counter-productive to their broader political aims.

We can see this in the IRA political activities (Sein Fein), where hardliners cannot be actively acknowledged (causing splinter groups – Real IRA) as it may endanger political negotiations and dissolve any goodwill developed by the current cease-fire. There are elements such as the Real IRA who will not *negotiate with the enemy* and they activity continue the campaign of violence. There is a real sense of irony that the political careers forged out of violence; often have as their first priority dealing with their former colleagues.

DOES TERRORISM WORK?

Governments and the media argue that terrorism doesn't work. History has shown that a small proportion of well developed terrorist campaigns *have* changed government policy, and the actual governments themselves. Groups such as the FLN in Algeria have gained independence for Algeria (from France); the Greek Cypriot group EOKA; even more recently the IRA has become involved in a fractious, but holding, power sharing arrangement.

Animal Liberation pressure groups *have* achieved some concessions in government policy throughout the Western world, even if the campaign continues.

CURRENT TERRORIST THREATS

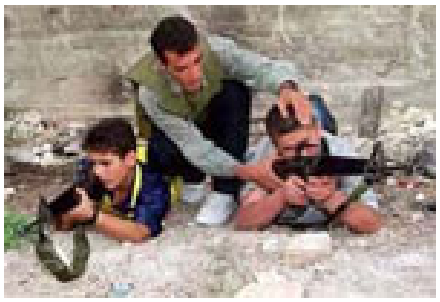
The nature of the terrorism has changed since the end of the Cold War. The West no longer fears acts of terror from subversive, Soviet-sponsored groups. America is currently enmeshed in a battle for the hearts and minds of the Middle East and mainstream Islam. A number of groups comprised of old allies like the Mujahedin, who helped fight the Soviets in Afghanistan have turned upon their one-time supplier of arms, equipment and funds. The disenfranchised and embittered led by the charisma, funds and determination of Usama Bin Laden and his Al Qa'ida operatives has staged a continued campaign to attack Unites States (and allies) interests around the world. The cause is said to be for Islamic religious freedom, but invariably this is demonstrated in a series of political demands (such as that of a Palestinian state).

The end of the cold war has meant a great deal of nuclear fissile material has filtered out of the decaying Soviet bloc, and turning up on black markets around the world. The fear is such weapons and material will be used to create Weapons of Mass Destruction, to broker greater leverage for terrorist causes.

A group who can be said to have used *Weapons of Mass Distraction,* Aum Shinrikyo, have already lifted the anti in terms of causing fear, by using Sarin nerve agents in Tokyo subways in 1995. The incident caused few deaths, but such acts can cause great financial losses for an economy and fear amongst the general populace. The Aum sect is one example of an apocalyptic religious group that is convinced the world is going to end, and can demonstrate this with extreme acts of violence (to reserve a special place in the afterlife). Such groups cause alarm, because a large number of people are under the direct control of one supreme authority figure, who may well become corrupted with such power.

State sponsored terrorism is prevalent around the world. Countries like Libya, Iran, North Korea, Cuba, Sudan, Saudi Arabia and Syria all have been stood accused of supporting terror organizations in recent years. It maybe said that countries such as the United States through the use of CIA, has used terrorist-like activities to achieve their aims around the world. Although technically, terrorism is an act by a non-political power – the difference can be a mute point to the civilians of the countries involved.

GUERRILLA WAR CIA GUIDE



The following summary is based upon CIA documents circulated during the 1980s in response to the Sandinista Government in Nicaragua and the creation of Freedom Commandos…

COMBATANT-PROPAGANDIST GUERRILLA

The guerrilla movement by its small numbers and lack of access to the media needs to foster the ability in its fighters to be both combatants and the catalysts for political change. Such factors include

- Improving the combat potentiality of a team by making all understand the motivations of the cause clearly and concisely
- The guerrillas should understand the link between the community and the political cause
- By gaining support of the local community, the group gains a psychological basis for their actions
- By developing trust with the local community, the group gains safety
- By promoting the value of participation in civic affairs, the group gains power
- By developing the persuasive face-to-face skills of each guerrilla the group wins the support of the population

GROUP DYNAMICS

To successfully change the regime of a country, first the guerrilla needs to internalize and understand the clear goals of the group, and understand the points of view of each other guerrilla. The weakest member of the current team is likely to train others at a later date, which may lead to the end of the movement. So achieving a high degree of cohesiveness within the group is a key goal structurally, it is also important in stopping any fracturing of the movement.

Usually, small groups are favored for such activities, as it is harder for opposition forces to infiltrate and/or destroy – especially if the intellectual basis for the change is ultimately directed from elsewhere. Smaller groups also lessen the problems of the pack mentality, if gaining the support of the local community is important – the less problems caused by pack behavior are favorable.

It is important to hold regular meetings amongst the guerrillas to establish a cohesiveness to thought and action. A political cadre (*a political leader*) should be appointed to facilitate such discussions, allowing others to speak – but ultimately framing the discussion in the ethos of the movement. It is important for the guerrillas to hold similar discussions with locals. Great importance should be directed to involving the team in the everyday affairs of locals, helping them to maintain crops, working upon civic initiatives and being present at civic activities.

Every guerilla should be able to respond with 10 logical reasons why the guerrillas cause is in the interests of local citizens, they should generally be easy to understand, and hopefully be firmly based upon everyday realities.

CAMP PROCEDURES

Each guerrilla force should at some stage be encamped away from the distractions of everyday life. It builds cohesion within the team, and trains them to deal with times when such actions will be done out of necessity, rather than leisure.

The leader should designate the following tasks

- Clean the camp area
- Provide drainage in case of rain, create trenches and holes for marksmen, dig a hole for the stove and build the stove (3 rocks placed around a hole and covered in with dirt and mud)
- Build a windbreak wall from common vegetation and camouflage
- Construct a latrine and hole where other waste can go (covered over when camp the is abandoned)
- Watchmen posted with 24 hour passwords, and relay the location of an alternative meeting point if the camp needs to be abandoned

Hopefully, an environment for focussed discussion will be facilitated, the guerrilla gradually becoming their own internal critic for the cause, even when hard times present themselves.

INTERACTION WITH PEOPLE

The basic underlying philosophy developed should entail living, eating and working with the local people. This should also extend to respecting their human rights and property, protecting them from harm and improving their basic skills (like read and writing).

ARMED PROPAGANDA

Many problems present themselves with freedom fighters carrying weapons and how locals perceive them. There is always the lingering doubt at the back of a civilian's mind of the implicit threat guns present. The best way is to maintain openly friendly greetings, putting aside the guns to help them in everyday tasks and the use of slogans like *"the weapons will be for winning freedom; they are for you"*.

IMPLICIT AND EXPLICIT TERROR

Along with the implicit terror of guns, citizens also invest in guns for safety – if the current government didn't keep them relatively safe through such displays of power, there would be chaos. Allow children to play and hold the guns, one can reinforce the ideology that the guerrillas are working for the people, and showing off the tools that will achieve it for them.

SMALL TOWN OPERATIONS

An armed guerilla force can effectively take control of a town through…

- Destroying local military and police installations and the removal of survivors to a *public place*
- Cut all outside lines of communication (cables, radio and messengers)
- Set up ambushes in order to delay reinforcements at entry points
- Kidnap all officials of the government and remove them to a *public place*
- Establish a public tribunal that depends on the guerrillas and promote it to the citizens
- Shame, ridicule public symbols of the current regime and humiliate persons of the regime
- Reduce the influence of the individuals of the regime, pointing out their weaknesses, and lead them out of town
- Take care to mix guerrillas into the public and make sure they are on their best behavior (paying for any articles taken, accepting hospitality and pay courtesy visits to other prominent person in town like priests, teachers and doctors)
- Instruct the population that in case of being interrogated by government agents to reveal everything they have witnessed for their safety
- Instruct citizens they can give names of government informers at discussion meetings
- Such meetings should be finished with a stirring speech by a political cadre who gives thanks to locals for their hospitality, dictate that enemy agents must not be mistreated and relate that the guerrillas appreciate the risks the locals run in supporting the guerrillas

LARGE TOWN OPERATIONS

In larger towns, it is unlikely that guerrilla activities could take control, but it may be necessary to use violence, the following concessions should be made…

- Explain to people that such actions are being done to protect them
- That the action is being performed as a *force of justice*, which the current government can no longer perform
- Such actions are necessary to secure the greater goal of freedom
- Explain if the citizen had escaped punishment they would have enacted greater deeds of violence
- The guerrillas were forced to act by the detainees actions

USE OF SELECTIVE VIOLENCE

It may be necessary to use violence against one particular target such as a judge (for propaganda purposes). The person should be chosen on the following basis…

- The spontaneous hostility of the locals
- An individual whose actions affect adversely a large section of the populace
- If the majority of the population have already given support for the individual, do not try to go against their wills
- The inability or ability to control the person who will take their public role

One must also consider the following factors…

- The degree of violence necessary to affect the change
- The degree of violence acceptable to the population to affect the change
- The degree of reprisals such an activity would solicit

The mission to replace the individual should be followed by…

- Testing the reaction of the locals, and control it to reflect favorably upon the cause
- Explain the necessity of the change and why it is good for the people
- Explain any possible retaliation would be unjust by the government

ARMED PROPAGANDA TEAMS (APTs)

Most groups should be comprised up 6 to 10 people, a leader should be selected and a political cadre should be appointed. All political cadres should have already been taken away for specific training in developing interpersonal skills, familiarity with the ideology of the cause and the ability to use emotive registers to control the thought and communication of the team.

One tool of use is the Interior group/Exterior group dynamic, human nature dictates that we form personal associations with people – aka the *us* and *them* mentality. By using the current government as them, or the *false group,* you can build a strong dynamic within the team. It is also easier for humans to be *against* something than for something; notionally being *for* something tends to suggest commitment; whereas being against something doesn't implicitly tie you down in your position.

We can also use Primary and Secondary groups to explain the relations of most humans. The primary groups consist of things like families, comrades and intimate friends, as opposed to Secondary Labor groups, like clubs and government organizations. By understanding this, the political cadre can attempt to bring the political message into the local's homes as a friend, and establish closer ties.

TECHNIQUES OF PERSUASION

Being simple and concise in expressions helps immeasurably to get across your point; hopefully this skill has been honed by hours of discussion within the guerrilla group already. But by using simple words and lively realistic examples the locals can get emotionally involved in the cause; impersonal political actions become personal goals. One should take note of non-verbal gestures and seek to harness them to the fullest, along with using vocal tones to emote the issues effectively.

EYES AND EARS OF THE POPULATION

Primarily the Armed Propaganda teams are deployed to gain the confidence of the locals, occasionally locals will supply the teams with pertinent information to the cause, usually the political cadre will report this along with the brief synopsis of the public reactions to propaganda activities to the chiefs.

PSYCHOLOGICAL TACTICS

The psychological tactics of operations are likely to change over a period of time, although the basic message will be preserved it may be important to genuflect it another way to gain the support of like minded organizations. The basic target population should however be chosen from the following considerations…

- The object is the people, *not* the population size
- The team should be able to cover up to 6 similarly composed towns
- The team should always move in a covert manner into towns
- They should always alter their route radically, but not the itinerary (hours of contact)
- The danger of ambush should however alter the itinerary a little, like arriving and leaving without notice
- Whenever surprise factors are used, one should use vigilance to detect the reaction of the audience (for hostile elements)
- No more than 3 days should be spent in any one town
- This 3 days helps reinforce psychologically that the information they have been given is present and up-to-date, plus staying any longer can cause overexposure of the target audience and possible negative reactions
- Basic tactical precautions should be undertaken to be discreet, such activities promote respect from locals for not endangering their lives
- The precautions should include - two individuals should meet at a prearranged point to scope out the meeting place ahead of time and after (to observe for hostile forces)
- The team goal should be to motivate the entire town, but still focussing on the target groups
- The political cadre should mix with the target groups before, during and after meetings to clear up any misunderstandings
- In the first meetings the political cadres should activity work to identify the key inhabitants within the town (in the focus groups) and help them out with daily tasks
- In free time the guerrillas should mix with the locals and participate in community tasks and social events (birthdays, parties, weddings etc)
- Cadres should be humble and respect elders and they should not immediately make their political aspirations known in the first phase

Tactical objectives to identify the cause with the local people include

- Establish identification through participation in local customs
- Determine the basic desires of the target groups
- Discover the weaknesses of local government controls
- Slowly forward the groups ideals into discussions

Special care should be applied in dealing with the local farmers or industry bodies, using the standard conceit that governments are hermetic organizations concerned with profit making and self interest. Intellectuals should be targeted using the discourse prevalent to their professions, perhaps using the criticism that the government doesn't allow for true free speech (censoring pertinent criticism).

The APT should not engage in violence if necessary, if the situation requires it, the use of overwhelming force should be used; if the enemy is larger, a tactical retreat should be hastily enacted. Dealing with such situations should be done with the utmost expediency (as turning the town into a battleground sends mixed messages, and the local will not feel their safety is ensured).

MOBILE INFRASTRUCTURE

The political cadre is the key to spreading the message to the local community, such an individual tied to a APT means that the entirety of the guerrilla movement will have a level of control and the ability for superiors to modify the message quickly as circumstances change. Additional, is the ability to receive feedback from the ground. Such units also allow for the infiltration of towns where regular freedom fighters could not enter (*similar in concept the Fifth Column movement in WWII*). Hopefully after some degree of discussion with the locals a number of key individuals are behind the movement.

DEVELOPMENT AND CONTROL OF FRONT ORGANIZATION

The infiltration of existing organizations whose goals are somewhat commensurate to the overall goals of the guerrilla movement is a handy way to gather a base to cause insurrection with. The added bonus is that the guerrilla movement can further their goals without necessarily laying its cards on the table.

INITIAL RECRUITMENT

Talking to a member of the target group without specifying the reasons why such discussions are taking place is a good way to co-opt an individual into your cause. Once the meetings have taken place, by forwarding information to the individual that the purpose of the meetings was to undermine the government, you can effectively black-mail them into the cause.

Once basic intelligence gathering has found suitable candidates for APTs, these individuals can be sent out on small missions to prove their allegiance to the cause. They can then be directed to join the relevant grass roots organizations like worker's unions, political parties, student bodies, youth groups agrarian bodies. Once there, they can provide feedback on other individuals who may be of interest to the cause. The individual should try to make an approach through an acquaintance and invite them for a dinner.

RECRUITMENT GUIDELINES

- If an informal conversation seems to suggest the target has similar beliefs to the organization, a political cadre will make the formal approach
- If the target seems not to be susceptible to recruitment, further meetings should be arranged with guerilla leaders – to blackmail them into the insurrection cause (as above)
- Police can be notified of hostile individuals through providing false statements of non-participatory members of the cause, with due care taken to not implicate the original contact
- Care should be taken to gradually build up the complexity and danger of clandestine missions for new recruits
- This technique should succeed in gradually infusing other organizations with key individuals for a time when outright civic protest will be actualized

Established Citizens, Subjective Internal Control

Once established citizens like doctors, lawyers, businessmen, landholders, minor state officials are on board the cause, they can be used to establish internal controls over their groups and associations. Once effective control has been achieved within such organizations, instructions should be given to…

- For internal cadres to use Socrates dialectic to denunciate oppositional voices
- The use of clear themes, words and thoughts to establish a process of thought
- Amplify themes of frustration through the motivation of financial profits and loss
- Underpin feelings of politics being an elite club, outside of the remit of the organization

Most intellectuals feel the government in some way doesn't use their valid criticisms to affect change – by showing this injustice and finding examples of censorship, it may be easier to target such groups.

The cadre should always seek to maintain a low profile within the group, so that the feelings seem to come *spontaneously*.

ORGANIZATIONS OF CELLS FOR SECURITY

Internal cadres should organize into groups of three within the target group, only one should maintain outside contact with chiefs. The three should have covert meetings outside of the organization, and seek to generate criticism of each other's actions, the provisional *senior cadre* reports back to the chiefs.

FUSION INTO A COVER ORGANIZATION

Once the basic structure of groups has been achieved and there is widespread support for the guerrilla movement it is necessary to convince disparate groups to unite under the banner of protests against the government. The internal cadres should begin to suggest the various reasons why the groups have mutual interests, that there is a better way to organize the government to service these interests. Hopefully, from this stage (with a little cadre direction and focus) the movements should naturally start joint meetings and develop stratagems to defeat the government of the day.

Meetings then should be openly held between groups, meetings should be organized between the guerrilla leaders and leaders of the front organizations, the groups should be encouraged to publish joint communiqués of the meetings. After which time, there should be enough momentum for the guerrilla movement to openly court regime change at mass rallies, and create a *whiplash* effect upon the population at large for change.

CONTROL OF MASS CONCENTRATIONS AND MEETINGS

Large concentrations of individuals protesting on the streets or large rallies create a powerful psychological tool for regime change.

INFILTRATION OF GUERRILLA CADRES

At this juncture of time, the trained soldiers of the movement should infiltrate the various front organizations to prepare for the charge towards open insurrection. Careful handling by the internal cadres should take place to make sure the more vigilant struggle activities are harnessed in a positive way.

Special care should now be used to recruit those segments of society that are vulnerable to recruitment (students, unemployed, minorities, laborers). Media propaganda at this time should be stepped up, and an even more strident message specifying the following…

- Describe the government as the negative image to the causes positive one
- Government entities enslave, not liberate people
- Police mistreat those whom they are employed to protect
- The government maybe a puppet to outside interests
- Taxes exploit, not benefit the people
- The working man is exploited by the rich

SELECTION OF APPROPRIATE SLOGANS

It is important to distill the ideology down into simple messages; words such as God, Homeland, Peace and Democracy are words that can prove effective. If such messages don't prove motivating enough – going back to partial demands like "we want food" might be necessary to establish the links to the appropriate *buzz-words*.

CREATION OF THE NUCLEI

After the first public rallies, a number of new guerrilla recruits will want to join the movement, these individuals are usually disgruntled with some actions of the government and should be hastily formed into groups under the command of the cadres, and set specific mission to complete. It may also be helpful to establish links with criminal organizations, who have skills of use to the guerrilla movement. Some criminals can even be hired to perform specific jobs. Cadres at this time should attend to travel plans for large numbers of people, and then go to employment agencies and *hire* unemployed people to be bussed to rallies. Others should be detailed to create posters, placards and get the relevant message to the communities. One can even create martyrs for the cause by sending them on dangerous solo missions, to further enflame public hostilities

WAYS TO LEAD AN UPRISING AT MASS MEETINGS

The use of some 200-300 agitators in a crowd of 20,000 can give the impression of a united movement, even if the people have attended originally under the behest of holding a peaceful rally. The operations should be carefully planned, taking into account the following structure…

Outside Commandos: These guerrillas will remain effectively passive, making sure that all high places like clock-towers and high buildings are utilized to keep watch upon the proceedings below – these troops are the eyes and ears of the operation

Inside Commandos: These troops are maintained in the crowd to protect leaders from harm, they will seek to avoid open hostility, and generally are assigned to keep close to specified placards in the crowd for easy reference

Agitators: Should be mixed in the crowd at specific placards, so the leaders can send messages to change the key words of agitation as they see fit. They will eventually seek to incite violence, and move on quickly, the cadres should then be dispersed to key points on the road for easy observation by the Outside Commandos, to ensure all are safe

Defense Posts: These people will be specifically assigned to maintain a protective ring around the leader/s at all times, and helping him escape if necessary – these should be guerrillas in civilian clothes and highly disciplined

Messengers: These individuals should remain near the leader to transmit instructions as necessary – they can communicate via radios, bikes, move on foot, cars ‘etc’

Shock Troops: These individuals should be armed with weapons and should march just behind the gullible and innocents participants. They will only enter into combat if the police attack the rally – their role is to provide a violent surprise, and give enough time for the leaders to disappear

Carriers of Placards: Special care should be taken for guerrillas to be assigned to individuals within the crowd carrying contrary messages, in this way the commander will be able to act if infiltration has occurred

Rallying Cries: The agitators should be able to direct the various cries towards the guerrilla groups aims, as most individuals in large crowds feel the group dynamic - which will generally override any personal feelings

INTERROGATION

The following summary is based upon a CIA briefing document for interrogators devised during the 1960s…

The basic skills needed by interrogators are…
1. Enough operational experience to sort out fact from fiction, and focus on the process
2. A real familiarity with the language the interrogation is taking place in
3. Extensive background knowledge of the interrogatee's country, culture and intelligence/military service
4. A genuine understanding of the source as a person

The interrogator should be selected from the pool of talent available, matching s/he for commonality and knowledge of the interrogatee – as rapport is of greater significance to achieving results.

The basic plan of the interrogation process

1. Identify the individual
2. Interview the individual
3. Research the individual
4. Determine whether the individual is likely to give up information under favorable conditions (psychological assessment of character, service ethic & knowledge)
5. Determine whether coercive or non-coercive measures need to be taken
6. Determine what information the individual is likely to know
7. Prepare a framework for the interrogation (targeting weak psychological points, demeanor, timeframe & approach to questions)
8. Interrogation
9. Debriefing report on information elicited and counseling for the individual
10. Possible further interrogations, depended upon debriefing report

It is important to understand an interrogation might not even be necessary, some individuals might well be at liberty to tell of the information needed freely. That is generally why an interview is held before any interrogation takes place. This interview helps establish the individual's bona fides, the basic story of any *walk-ins* and afterwards, the general psychological state of the interviewee can be assessed.

The basic process of interrogation is to determine under what circumstances the individual will give up specific outlined information. By using more threat or pressure than is necessary, one can actively turn a willing subject into a hostile one.

THE INTERROGATEE

The first consideration is classifying what particular type of intelligence source the individual represents, it is important in understanding their particular motivations and the amount of time and effort the individual should represent.

Types of Sources

1. Travelers
2. Repatriates
3. Defectors, escapees and refuges
4. Transferred sources (from friendly foreign agencies)
5. Agents (Provocateurs, Double-Agents, Foreign Agents, Service Agents, Swindlers & Fabricators)

It is especially important to understand that agents have different specific motivations, a provocateur seeks to take up as much time as possible, whereas a double-agent could well be seeking to pass on fraudulent information at the debriefing.

PERSONALITY CATEGORIES

There are generally two paths to understanding the individual, one uses geographical-cultural references, the other, seeks to use psychological-emotional emphasis. It is best to understand the individual is a product of both forces, and to proceed accordingly – but understand these are analytical tools. There is no substitute for establishing real empathy with the individual.

The following list of the nine major groups of psychological-emotional states represents a basic analytical tool for understanding human motivations.

The Orderly-Obstinate Character: This type of person is characteristically cold, frugal and orderly. They may well be intelligent, and use their intelligence to set up an outward façade of civility in adulthood. Underneath, they are highly suspicious of authority and assert their individual desires around learnt traits of passive-aggressive behavior. They are secretive and may harbor desires of overthrowing authority/ authority figures. They are stubborn and their system of morality is unshakeable. They maybe fastidious and be particularly enamoured with personal possessions (like trinkets and keep-safes).

The interrogator should proceed with caution and avoid threatening gestures and projecting the role of a hostile authoritarian. Establishing rapport is extremely important when dealing with such individuals. Dressing neatly may prove rewarding. The individual may confess easily under the right conditions – given their feelings of guilt (which may even include acts they did not commit). Flattery may prove beneficial.

The Optimistic Character: The defining characteristics of an optimistic character are that they are happy-go-lucky, impulsive, inconsistent and undependable. The individual may be generous; they may have addictive personalities and run from pressure situations (to avoid conflict). They avoid responsibility for their situation by believing that good will impact upon their lives ("something will turn up"). They have usually been overindulged as a child; they may be the youngest of a large family. Due to severe frustration in adolescence they may be petulant, vengeful and demanding.

The interrogator should adopt the characteristics of a kindly parent. Pressure tactics or hostility will force them to retreat internally. They tend to seek promises, and cast the interrogator in the role of protector – it is important not to make specific promises, as they will tend to turn vengeful in response.

The Greedy, Demanding Character: This type of character tends to affix himself/herself to an individual like a leech and clings obsessively. Although the subject is dependant on others and is passive, they constantly demand the host to gratify their wishes, and defend them from outside harm. If the host is seen to let them down, they will seek out another host.

The greedy, demanding character is generally established in childhood or adolescence, when they have been deprived of parental care – in adulthood they seek out substitutes that will.

The interrogator should attempt to adopt the demeanor of a father or big brother, and never seek to rebuff the individual (for fear of destroying the rapport). The interrogator must not accede to exorbitant demands, but doing an unimportant favor could be a necessary substitute (they are generally seeking reassurance and security, not a specific item).

The interrogator must be careful of using logic and rational persuasion; the individual may well have a worldview firmly altered by experience – it maybe necessary to use their own emotional registers upon them, than pure reason – their emotional resistance can only be dissipated through emotional manipulation.

The Anxious, Self-Centered Character: This type of character is stereotypical of a thrill-seeker. They are in a constant struggle with their concealed fears, and compensate through pretending they have no fear of such activities. They may well be a Don Juan, challenging themselves. They tend to brag and often lie through a hunger for approval or praise. These anxious, self-centered characters are usually vain and equally sensitive.

The interrogator should be aware of the vanity of the subject and play upon their weakness (praise and fear). By not admonishing extravagant personal lies, the interrogator can make the vain subject open. By establishing the safety of the individual and promotion of the *folly* of the subject's superiors in sending them on such a hazardous mission can reap results – one will hopefully have optimum conditions for extricating the truth.

The Guilt-Ridden Character: This type of person has a cruel, unrealistic conscience, their lives are in a constant state of flux between reliving feelings of guilt and apportioning the blame onto others. They seek at times to provoke unjust treatment in others to assuage personal feelings of guilt. They are often compulsive gamblers, who often get more satisfaction from losing. These people will often admit to crimes they didn't commit, or indeed, commit crimes unconsciously to confess and be punished. Masochists also belong to this category.

The guilt complex often forms from relations with parents and others in childhood, who they felt have wronged them – or actually wronged. As children they may have been frequently scolded or punished, they feel they deserved love and honor instead. They may also have been 'model' children who repressed all their natural hostilities to authority figures.

The guilt-ridden individual is often hard to interrogate. Understanding their need to confess for any clandestine activities, one should treat all information with care. The individual might often confess with provocation, or remain intensely silent (enjoying the punishment). It may often be necessary to punish the individual in some way, to play out the moral preoccupation with guilt.

The Character Wrecked-By-Success: This characteristic is closely related to guilt-ridden characters. This person subconsciously avoids achieving goals in life by sabotaging their activities. The person will only enjoy the fantasy of ambition, but will find ways to avoid reaching their destination. It actually stems from a sense of guilt, that they are not worthy of the success. The individual will often seek to project their guilt towards other people, blaming them for their failures. The individual has a strong need to suffer, and may actively seek danger. They may also be accident-prone. The individual feels they are incapable of indulging in pleasure and accomplishment.

The interrogation of such individual's pose no particular problems for the interrogator, unless the interrogator makes unwanted moral judgements about the subjects lack of success. The success of the interrogation might be enhanced if the interrogator is aware of the events in the subject's life that strongly project this level of failure/guilt, and actively avoid broaching them.

The Schizoid Character (Or Strange Character): An individual who lives in a fantasy world much of the time. The schizoid character is sometimes unable to distinguish between the real world and their fantasy one. The individual may have symptoms of Borderline Personality Disorder – find the real world empty and meaningless, place undue significance to conspiracy theories and have no real empathy for others. This type of character maybe extremely intolerant to normal everyday frustrations, and cope by withdrawing inside themselves. They may attach symbolic meanings to others.

Children reared in homes lacking in affection or attention (such as orphanages or state-run institutions) may grow up to be part of this category. At some stage they have been rebuffed for early efforts to attached themselves to others. They grow to distrust others and turn their minds inward. They will still actively strive for external approval, but the damage done at an early age will retard their abilities to respond in an appropriate manner.

The interrogatee will initially strive for acceptance of the interrogator by fabricating lies that they feel will appease their captor. It is prudent to understand the fantastical nature of some of the intelligence gained, and seek to clarify the truth by complimentary questioning. The interrogator can use the desire for approval as the handle to orchestrating discussion. The truth may be gained by assuring the individual no harm will become them (being their main concern). Such characters are particularly unreliable for turning purposes.

The Exception: These individuals believe the world owes them a living, they are highly demanding. This usually stems from a childhood incident where an injustice has been seen to be perpetrated upon the individual (death of parent, deformity, major illness). The individual feels they are deserving of a good turn from fate, usually through their dealings with others. If their claims to privileges are ignored, they may become rebellious like an adolescent.

The interrogator is likely to be confronted by a list of demands for their cooperation, usually out of proportion to their contributions to knowledge. Any ambiguous replies from the interrogator are likely to be seen as acquiescence to their demands. The interrogator should actively listen to their demands (time limits set), and dispense any concessions that are within their power. This type of individual is unlikely to make a good turned agent, as their priorities lie with themselves primarily.

The Average (or Normal) Character: These individuals show various elements of the above categories, but tend to be a blend of fears and complexes. The average human under interrogation will be shown to have qualities of obstinacy, unrealistic optimism, anxiety at times. Their reactions will generally be balanced to the level of threat posed by the questioning, and be constitutive of the questions remit (not being constitutive of psychological complexes).

Other Clues: True defectors are likely to have a history of active opposition to authority and therefore, are likely to rebel against their new authorities.

SCREENING & OTHER PRELIMINARIES

The basic idea of a screening interview is to establish the identity of the individual, ask basic questions about them and to determine any pertinent psychological clues through responses. Even an agent provocateur is likely to go beyond their legend and reveal traces of resentment through questions about authority figures, and use autobiographical information about their childhood through the interview process. The interviewer shouldn't be the individual who will be the interrogator, and best results will be obtained through the interviewer imagining the mindset of the subject. Hopefully, the subject will have revealed some key psychological issues, which can be exploited if an interrogation is necessary.

PLANNING OF INTERROGATION

It is useful in planning an interrogation to point out reasons why a subject will ultimately give up information.

1. The person is accused explicitly or implicitly and feels accused
2. The individual feels their psychological freedom is curtailed
3. The individual is defensive because they are unsure how much their captor knows, making them uneasy – and unable to formulate a stable psychological position
4. The individual senses a great disparity between their own power and the accusers power, even perceiving that the accuser has real evidence. This being an untenable position psychologically
5. The individual believes they are beyond the help of friendly forces, and they are their only source of salvation
6. The individual feels guilt, otherwise they will actively resist until severe duress
7. The individual is pushed so far that it is easier psychologically to acquiesce

In planning, the interrogator should understand that the individual needs a firm rationalization for giving up such information (hopefully based upon their psychological needs). That the subject has been wronged by the foreign intelligence service, that there is no disgrace in revealing information under duress, that they are ultimately more important than ideology.

The basic tenant of interrogation is to regress the individual's psychological state, to strip them of their adult coping measures and back to an infantile state. This is helped by removing the individual's liberty to leave, removing their clothing and personal effects and having interview rooms blank (without everyday objects). The isolation helps to break down the individual from their everyday realities – it is extremely distressing for well-adjusted people to be removed from the world at large, as they are keenly interdependent upon the nourishment of social interactions.

Recording devices should be concealed within the room, the room should be soundproofed, and the less distraction within a room will focus the mind of the subject. The interrogator should have defined all the necessary questions ahead of time and visualize any particular problems that may lead the interrogation to go off-track.

It maybe prudent to have more than one interrogator present, it may prove effective to alter the timing of interrogations and detentions of the subject (to disorient the subject). Finally, the interrogator should plan to finish the interrogation in a way that doesn't leave the subject disgruntled (if they are needed in future).

NON-COERCIVE INTERROGATION

Non-Coercive Interrogation refers to the generation of pressure upon the subject by mere words alone. They seek to manipulate the subject psychologically, to make them compliant. Some tools include

- Thick File: Convincing the subject that a large, thick file produced is a file on the subject (false assumption)
- Detention: The interrogator is at liberty to control the subjects environment
- Human Contact: The interrogator can limit the level of human contact to the subject
- Questions: The interrogator sets the agenda
- Time: The interrogator determines the time the subject is incarcerated and interrogation times
- Consumption: The subject can be denied meals and water

By manipulating the environment of the subject, the interrogator can be seen as an authority figure, or a benevolent friend (who has under their control the possibility of salvation).

STRUCTURE OF INTERROGATION

1. The Opening: The interrogator seeks to establish a rapport with the individual, hoping to avoid the problems of a lack of understanding, allay resistance from social conditioning, allay beliefs that the information sort will damage the subject and that the interrogator is hostile to the subjects ideological beliefs. It is also used to confirm if the psychological assessment is accurate, it may also be important to let the subject speak freely to get an accurate idea of their mannerisms while under less stress.
2. The Reconnaissance: This interim stage is necessary if the interrogator meets resistance, the interrogator will seek to probe probable areas of resistance and gradually focus upon resolving them. It is important not to get frustrated and make it a personal contest – even resorting to ruses to circumvent such resistance.
3. The Detailed Questioning: The object of the interrogation starts, the interrogator must fashion questions that get to the point of the interrogation without revealing the informational gaps in knowledge. It is useful to divine if the individual's knowledge is first hand or through an intermediary. It is important not to become brusque in one's questioning, and possibly loose the rapport.
4. The Conclusion: It is important to reestablish some degree of rapport, and establish a creditable motive as to why the subject has revealed such information.

TECHNIQUES FOR NON-COERCIVE INTERROGATION OF RESISTANT SOURCES

1. Going Next Door: The information sought might actually be readily available from another source, who is already compliant
2. Nobody Loves You: The interrogator lies that other sources have provided incriminating confessions that the individual is the culprit, hopefully anger and futility will spark the subject to reveal information
3. The All-Seeing Eye: The interrogator tells the subject s/he knows all, and the purpose of the interrogation is to determine the reliability of the individual. The interrogator starts with information already known, and seeks to catch the subject out. After a few questions the interrogator can slip in questions of unknown facts. This ruse will ultimately fail if overused
4. The Informer: The planting of an informer in the cell where the subject is held can be useful. A further technique is to use two informants, Informant A tells the subject that Informant B is an informer – even finding a microphone planted in his/her bunk. Hopefully, the subject will confide in Informant A
5. News From Home: Allowing the subject to receive selected letters from home, and establishing that letters can be smuggled out – can extract information surreptitiously
6. The Witness: By establishing the existence of another fellow spy, one can pass one by the other on the way to the interview room. An hour later, the two can be passed quickly by each other to avoid contact, and a stenographer can appear from behind the door clutching a folder, asking for the subject's name. Which can cause doubt in the unwilling subject's mind, as to whether the other has talked or not. Modern recording technology can be use also to splice together phrases of a *confession* which may also have the same effect
7. Joint Suspects: If two suspects are taken together it may be appropriate to keep them separated for a week then interrogate them, playing upon their natural fears of being exposed by the other. Once the interrogations take place, producing a signed confession by Suspect B to Suspect A (a document containing enough salient facts of the case firmly focused upon placing the blame on Suspect A). This might invoke Suspect A (hopefully the stronger psychologically) to give in and relate the real operational facts. Another ruse, can be the weaker suspect (Subject B) can be placed in the interview room, Subject A placed just outside the interview room waiting to be interrogated – eye contact hopefully being established between the two. Another person takes Subject A momentarily away to fill out a form in another nearby room, Subject B is whisked away from the interview room, whilst the interrogator continues to get louder inside the interview room. Subject A is taken back to the waiting area just outside the interview room – now the interrogator can get louder (aka audible to outside) and make believe Subject B (no longer present) is actually breaking under stress. The interrogator then pops his/her head out the door, and goes ballistic at the administrative flunky for placing the other suspect just outside, and demands Suspect A is lead back to the cells. It may also assist if sound recordings are taken of interviews, and spliced together (manually or electronically) to give the impression of a confession
8. Ivan Is A Dope: This involves pointing out that the cover story the hostile agency has contrived is ill-conceived and endangered the agent life unnecessarily. Leading to appeals that the interrogators organization would treat the detainee far better
9. Joint Interrogators: The typical version being the Mutt-and-Jeff (Good Cop & Bad Cop) scenario where one is domineering and uncaring, the other is comparatively friendly and empathetic (aka friend or an ally). This generally works best on the timid. It may be appropriate for the domineering interrogator to interrupt the empathic (starting) interrogator part-way through the process, and proceed to brazenly demand information. After pretending to lose his/her cool, the original, passive interrogator will direct the other to leave the room for a short while. Hopefully, the detainee will now take the opportunity to bear their soul to the friendly interrogator. The same technique can also be used by a single interrogator, starting out with a series of brutal interrogations in Spartan surrounds: the action can then be shifted to more comfortable surrounds, where the interrogator can be more friendly and divulge their prior actions were the dictates of command, and they regret their savagery. The detainee will usually feel a great deal of relief and camaraderie towards his/her interrogator, and may well tell their new *friend* information. Finally, another ruse is to have 2 friendly interrogators, one sincere, the other pretending to be sympathetic

10. Language Shift: The use of quick fire phrases and accusations in the bilingual tongue of a detainee might provoke unconscious admissions. The use of the detainee's lesser known language might also expose unconscious admissions. It is important though that the interrogation to always use a language they are proficient in
11. Spinoza & Mortimer Snerd: Most organization structures rely upon giving people just the right amount of information that is necessary to perform their tasks. This can be used against detainees. An interrogator can ask a series of questions that they know is beyond their level of knowledge, eventually a question is asked pertinent to the detainee, which they will generally answer with relief
12. The Wolf In Sheep's Clothing: Used primarily to expose double-agents, an unknown superior is substituted as a hostile superior, and a ruse of capture is played out – an *escape* is usually factored into the scenario
13. Alice In Wonderland: The basic premise is to ask *gobble-de-gook* questions, lowering the vocal deliveries pitch, tone and volume – making sure that no discernable pattern develops. Over time, the detainee will move beyond sheer denunciation of such stupidity, and realize such actions start to become mentally intolerable. Eventually, a sensible question is asked. It is especially effective against Orderly, Obstinate characters

REGRESSION

Manipulation of Time: Of meals and interrogation times will destroy notions of order and identity
Rewards: Giving rewards for non-cooperation distorts moral judgements
Relay Questioning: Getting two or more interrogators to continue long interrogations
Placebo: Give the suspect sugar pills and call it a *truth* serum, which maybe an excuse for their compliance
Hypnosis: Whether real or not, the individual may react similar to taking a placebo
Polygraph: The same basic deal, a justifiable reason to comply

THE POLYGRAPH

There is continuing controversy around the use of Polygraphs; it may be of some use as an aid to basic screening activities, but serious doubts exists about the absolute veracity of specific answers. The basic problem lies in the fact that questioning presents its own challenges; if you do not know the specifics of the operational activities/life history of the detainee, you may well frame a question in a way that it is *more* stressful for the subject to admit to the truth, than to lie. Evidently, tests have shown that an individual who has been trained to observe detainees and discern the veracity of their responses, is *better* able to tell the difference.

COERCIVE INTERROGATION TECHNIQUES

The basic theory for the use of coercive techniques is that the individual will not tell information without outside sources of pressure. It is vitally important to realize that using the right tool, for the right detainee is important. Most detainees are unaware how much pain they can actually take, if the threat is carried out, and they resist it – the detainee will sense a small victory has been won. Therefore, the importance of maintaining the threat for as long as possible is crucial.

The process is designed to cause *regression*, the thin veneer of self we call our everyday personality is constantly being reinforced by our friends, jobs, language, possessions and social structures. It is hoped through interrogation, the link between the detainee and the outside world is stripped, along with the coping mechanisms we develop to deal with the lack of control we have over others. Under the interrogation process, similarities exist between the parent and adolescent relationship, and the interrogator and detainee one. The interrogator has the ability to provide satisfaction and punishment, but the detainee has some level of self, and can maintain it under such pressures. Just as we may have hatred for our parents at times, feelings of warm may just as well develop between the interrogator and detainee. The constant pressure put upon the detainee is likely to result in feelings of *guilt* being established, even if the detainee hasn't done anything wrong, the parental-type role established by a good interrogator evokes such relationships. The ambivalence of the role helps to establish the guilt patterns – the rebellion against a kindly authority figure being both forgivable and futile.

The basic responses to coercion are debility, dependency and dread. The detainee will have a reduced viability as a functioning human, they can become hopelessly dependant upon their captors and experience extreme fears and anxieties. This state can lead to long-term apathy, which may be counter productive to gaining information – some measures should be undertaken therefore to ensure that the detainee believes that the information is the only stumbling block between them and release.

Extreme coercion may lead to profound psychological damage, cautions should apply, however, unless court activities will take place later it is entirely possible to push a person beyond reasonable controls and obtain the information required – the only problem maybe that the victim is less able to make fine distinctions in judgement.

Once the individual's resistance is broken down, it may be a temptation to personalize the activity and the interrogator can begin to gloat at *victory* – this temptation should be avoided at all costs. Such actions hinder the process of building a face saving reason for the compliance by the detainee, and will cause resentment to build in the individual who, at a later time, might yet again be called upon to provide further information.

PRINCIPLES OF COERCIVE INTERROGATION

Arrest: The individual should be arrested at a time when they least expect it, usually early mornings or evenings, hopefully, this will mean that they are less able to rouse their senses to defend against allegations and supply pertinent information

Detention: The individual upon arrival should be divested of all possessions, clothes, possibly cutting even their hair and issued with new, ill fitting prison garb. This helps to break down their individuality. Further, the detention area should be stripped of all references to the outside world, and be devoid of comforts. Any routine should also be avoided, having irregular meals, guards and interrogations. The individual after a few days will become stressed and look for some kind of order, which can be manipulated by the interrogator.

Deprivation of Sensory Stimuli: The removal of all stimuli from the surroundings of the detainee accelerates the process of removal from the everyday reality. By making a cell soundproof, lack in distinctive textures and colors and other individuals, relatively social people will quickly become anxious. This anxiety can drive an individual to start to delve inside their psyche and develop false connections with their environment. A trained interrogator can promote in the individual's mind the link that the interrogator is the source of their anxiety – and can lessen or increase this dependant upon cooperation.

The individual over time will be forced to regress to child-like behavior because their learnt techniques to deal with the real world have no place in such a non-linear environment, the problem is dealing with the unnecessary trauma such a time in their lives may reveal.

Threats & Fears: Threat is a far more potent tool than coercion, people generally underestimate their ability to handle pain. Threats aid regression, violence can be seen as a relief – and the individual may gain confidence from holding out so long. The detainee must always be aware of the purpose of the threat, if information is forthcoming coercion will not be necessary. Threats should not be delivered in anger, or as retribution for angry responses of the detainee – threats delivered in a cold distant voice by an individual believed to have the capacity to carry out such action have far more power. This also helps focus in the mind, the continued purpose of coercion – it isn't personal, it's a process.

Debility: It is often thought that subjecting a detainee to extremes of heat and cold, and depriving them of food, water, comfort and sleep will force them to capitulate – nothing is further from the truth. You are trying to break the mindset, not break the body. The proper use of these environmental factors is to break up their availability. People who are constantly deprived of sleep get used to such deprivations, but letting them sleep 12 hours one night, and waking them up constantly the next for ongoing interrogations is far more disturbing mentally. Obviously, there should be some controls, which are seen to be the sole responsibility of the interrogator (who can grant favors for compliance or take them away).

Pain: Although tests have shown all humans have the same threshold for pain, a number of factors contribute to its application in interrogation. An individual who has experienced pain when younger may be highly susceptible or be able to withstand great degrees of pain. Some people can handle great degrees of pain if it is seen to be inflicted upon themselves by another, but may find it harder to withstand if they are led to believe their resistance to talk has forced it upon others. Some prisoners feeling guilt can actually feel cleansed of their sins by enduring such pain, they believe they deserve it and it is going some way to relieving themselves of the burden. Persons with considerable moral or intellectual stature can interpret such use of pain as validation of their superiority to their captors. Finally, the use of coercive techniques late in the interrogation process can be interpreted as a sign of desperation on the part of the captors.

Excessive pain can lead to some captors making false confessions to avoid further distress. It can lead to a number of costly delays whilst facts are verified, indeed some prisoners given such time are likely to make up even more elaborate confessions to stall for further time. It is often best policy to avoid causing pain from the outset, as it makes all further attempts harder to implement.

Heightened Suggestibility & Hypnosis: The use of hypnosis is highly problematic in an interrogation sense. Firstly, the individual has to be willing to undergo hypnosis – the only way to get such cooperation would be the substitution of a friendly face. Secondly, the individual is quite able to lie under hypnosis, the individual's morality and worldview would be preserved – indeed, they are quite likely to *lie to themselves* in the sense of our normal everyday prejudices affecting our clear judgement. Thirdly, the enterprise necessitates a professional hypnotist; interrogation isn't an enterprise done by amateurs – as it can do irreparable harm.

On the plus side, if one can get the cooperation you can use post-hypnotic suggestion to operational benefit. One can even use hypnosis as a ruse; telling the captive they have ingested drugs that heighten their suggestibility to hypnosis and gradually increase the dosage until they pass out – when they wake up the interrogator can bluff that they have certain information, suggesting it would be in the captives interest to give them the rest.

Narcosis: Once suggested, 30-50% of detainees will believe a placebo sugar tablet to be a *truth drug*. In the reverse scenario, the use of real drugs can not guarantee absolute truth. Indeed, average well-adjusted people are more likely to get away with lies than a guilt-ridden neurotic one.

The use of drugs is still a valid concept, some people burdened with feelings of guilt and shame can relax a little more and start talking. Others may feel that once *truth drugs* have been administered that it is a valid excuse for admissions. Some drugs with highly hallucinogenic effects should be avoided, although it may expose some more extreme personality traits; it can also lead to fictitious additions to information. Matching the drug to the individual personality should be discussed with a trained doctor.

Detecting Malingering: During the interrogation process some individuals will undoubtedly fall ill or become mentally unstable, the following information should help to delineate between genuine cases and those feigning.

The average person generally knows little about real diseases of the body and brain; their knowledge is based upon movies of extreme cases. It is often believed that one symptom of delusion is that one believes one is a powerful historic figure – rare in true psychosis. The development of schizophrenia in individuals has a long onset time; such delusions do not spring up overnight. True schizophrenia rarely involves powerful dramatic shouts and gesticulation – such individuals have temperate moods just like anyone else.

Malingerers will also attempt to evade examinations by professionals by organizing circumstances. When a psychologist is present, they will generally focus upon the signs of illness *not* present as much as the symptoms on display – people with real psychological problems will generally flinch from such investigations. The use of drugs upon individuals with amnesia leads to the symptoms to momentarily disappear, unlike those in malingerers. A trick that can be played here is to show concern, and *believe* the individual is gravely in peril and ask for urgent electro-shock therapy, or a frontal lobotomy.

14. COMMAND HEADQUARTERS

This section will hopefully provide some general advice for the potential Games Masters to help run a successful campaign of the Spook Engine. As such, the following section of this book is only of real benefit to the Games Master…

ADVICE FOR RUNNING THE SPOOK ENGINE

Discuss Your Options With Your Players: I advise the best way to get people to appreciate your game is to discuss with them up front what they want. *Chapter 3: Setting Advice For Players* is meant as a handy reminder to players they have some input into the type of game that will be run. It doesn't mean they dictate the terms of the campaign, but have some say in proceedings. I find having an understanding of your audience needs helps you orchestrate your own ideas more successfully. The Spook Engine has a number of different options for game play; you should be able to find a setting and a group of character templates to everyone's liking. In the planning of a game, I personally find it rewarding to discuss with my players ahead of time what kind of game they would like to be involved in. If you are anything like me, there is generally a gestation time between the thought and the actual running of a campaign – it generally allows time for the basic premise and the campaign outline to suggest itself. If you discuss ahead of time the options with your players, they may well suggest some interesting possibilities that might not have occurred to you – and you can take all the kudos when they have forgotten and enjoyed.

Planning: Once you have the basic premise for the campaign or a one-off adventure, I find it best to do a little research on the topic. If I say, have a missing Russian warhead central to a plot line, I will usually hit the web and find an image and some basic background information. This 5 minutes of searching will give me a basic understanding of the particular type of missile that has gone missing and generally gives me a picture to show. If you accumulate data this way, you can achieve your objectives in a thrice, and obviate the need for delving into heavier, tierce tomes.

Sketching Out A Campaign: Once you have decided that your players are say, hired assassins, you can start to sketch out a world around them. Are the team freelance? Are they based in a particular country? What are their motives? From this basic core you can start to build a team of supporting characters, organizations and missions. It is important not to be too regimented in planning - like week 5: *they will be here, doing this*; players do not like being dictated to. It might make it easier in the short term to plan your campaign in detail; but your players will resent not having at least *some* free will. Although it may be stressful for a Games Master to relinquish a little control over the flow of the plot, it can ultimately prove rewarding (and spring interesting character-driven conundrums).

It can be daunting for a new Games Master to know when enough planning is enough; I personally find it rewarding to have the basic information about the organizations involved at my disposal, having important supporting characters sketched out, some material on any key vehicles/weapons/technologies used, a basic understanding of the locations used (and roughly sketched map). A basic timeline of events can also prove useful.

You will find that players often respond better if you have pictures of the major supporting characters, locations, maps and items of interest at hand. Players love props, and it infers a strange kind of credibility to the Games Master – players equate props to pre-planning effort.

Helping Players Create Characters: It is often tempting to let your players go solo in creating their characters and working with the team that eventuates. The character creation system employed in the Spook Engine doesn't take much longer than 10 minutes to complete; giving plenty of time for consultation with your players in a standard game session. What you primarily want is a fully formed character; it will make it easier for the player to roleplay effectively and make your job of presenting a realistic conflict more intuitive.

The fact is modern personal computers can run 3D action games that recreate the world of covert operations with more excitement and zing than any roleplay system ever could, what they cannot do however, is provide the *psychological* experience. A Games Master should play to this obvious strength.

What makes your team want to risk their lives for a cause, or the dollars? Why do they fight as professional soldiers for king and country? How precisely do spies exist in a world of such moral ambiguity?

If you want your players to turn up every week, helping them to discover the deeper complexities of their character will help them *care* about their character – and they will more likely than not, turn up every week. Think of television characters that are beloved, how much more tied to the experience would someone be if they have developed that character? Perhaps you might discuss with the player their favorite fictional character and why they like them? The basic dynamism of that character can usually be transmuted across to any scenario, even if the player isn't that interested in the current plot line, they can still have fun working through the character premise.

Player Driven Gaming: Some of the different character templates suggest a more *player driven* plot, meaning players are a little more proactive usually developing their own goals. A paramilitary group may well have a great deal of autonomy over their actions, whereas a special operations soldier would likely be reprimanded for not following orders. In terms of spies, an external spy will likely have a basic roving remit to gather information in a hostile country, whereas an internal security service spy will not. It is something of interest to discuss with your players. Some players quite naturally enjoy the experience of setting their own agenda, but others may struggle and need their superiors (aka the Games Master) to set specific missions.

ADVENTURE SEEDS

The following breakdown should provide with some initial ideas for potential scenarios…

SPIES

Internal Security

- A government minister's teenage daughter has being held hostage by extremist paramilitary organizations for 2 months, and *Stockholm Syndrome* has taken hold; with the daughter becoming convinced of the merits of the struggle – the daughter must be recovered unharmed
- The security service has been infiltrated by hostile agents and the team is deployed with a short list to find the suspect/s – with the potentiality of blowing the cover on a web of legitimate agents and officers
- A brutal murder of prostitutes leads to an uncovering of an illegal trade in human cargo and virtual enslavement by organized crime
- A local cleric is concerned with rogue elements within the local mosque preaching extremist doctrines, leading to potential suicide bombers being brainwashed into subservience
- Pirate broadcasts across local multi-lingual radio services warn of a terrorist nuclear attack on a major metropolitan city – time runs out for the team to track down the device whilst citizens vacate the city

External Spies

- The team is required to do close reconnaissance/infiltration of a highly patrolled nuclear power station, located at a windswept hinterland far from the major population centers – turning out to be a full scale weapons production facility
- The team is required to infiltrate a foreign extremist group and participate in activities and operations that undermine the state – whilst keeping their own cover
- The team is to kidnap a foreign attaché who is in possession of a military prototype device on route to their home country through a neutral one
- The team is to disguise themselves as hostile foreign spies and rendezvous with a suspected errant home agent and attempt to turn him/her – and tracking down any suspected intermediaries with evidence of complicity
- The team is directed to assassinate a hostile foreign General planning a coup to overthrow a compliant President/Prime Minister – possibly leading to information suggesting that another foreign power has backed the General

SPECIAL OPERATIONS

- A military junta has taken over key installations in a border town, the team needs to do close target reconnaissance and decide appropriate actions before more foreign troops reserves flood the town
- A diplomatic helicopter has crashed in disputed territories carrying vital strategic information needed for peace negotiations – the team have a 5 hour window to recover the said documents
- An embassy party on home soil has been attacked by separatist rebels demanding immediate action on injustices to their people, the hostage situation is complicated by important foreign nationals being present – the team is required to take immediate action with optimum precautions to avoid a diplomatic incident
- An oil rig not far from the coast is subject to denotation by terrorists, the team is scrambled to save the lives of drowning and trapped oil workers still on the platform – little do they know timed bombs still present have not detonated
- The team has been detailed to keep the perimeter fence clear at an emergency summit between government, military and secret service officials. A viable threat has been identified, which is currently taking advantage of insiders to plan an attack on the meeting location

PARAMILITARY

- Opiates must be trekked across guarded borders to meet up with a dangerous warlord and his agent, who has promised to supply arms in payment – little does the team know they are walking straight into an ambush
- The cells of the local secret police station currently house the leader of the local resistance movement, it is your job to make an assault upon the station and help exfiltrate the leader over the nearest border
- The local resistance movement has been blown, it is the team's job to recover the hidden weapons cache just outside of town before evacuating
- The military have located the movement's hidden forest enclave, your team has been detailed to protect the women and children whilst trekking across mountainous terrain to a relatively safe cave
- Foreign intelligence agents have made it known of their support for your groups activities, it is up to your team to make the advance, discuss the terms of any support and consolidate the arrangement – however a mole within the group is about to undermine the efforts

BODYGUARDS

- The vain, rich son of your client openly courts the wrath of local warlords, it is up to the team to make contact with the warlords and make peace (through financial settlement or otherwise), whilst still making sure of the safety of the client's immediate family
- After taking on a new client and his security retinue it is up to the team to vet the current employees and make changes the security detail – before internal fighting threatens the life of the employer
- The deposed Prime Minster/President returns to his fractured state looking to bring the rule of law to her disillusioned people – the current junta however have other ideas
- After the kidnap of a client by rogue elements of the protection retinue; after hospital treatment the team vow bloody revenge on their former comrades and hope to deliver their kindly client from their bondage
- After a bloody coup, the lives of all those supporters of the old regime (including the bodyguards of the President) are forfeit – the irony of bodyguards protecting themselves barley registers as the team engages in firefight after firefight heading towards the safety of the border

MERCENARIES

- The local military junta will pay a handsome bounty for anyone finding and killing the sons of the dead King
- A global oil company seeks to quell the local peasant uprising and occupation of a river mining site, your team is unofficially/officially at liberty to use what ever methods seem appropriate to break their embargo – although excessive loss of life is deemed *difficult*
- United Nations inspectors are about to make an appearance in the newly formed democratic state, despite appearances to the outside world the state is run by a fascist regime actively seeking to quell dissent – the team is deployed to make sure the locals live in fear of their lives; not telling all to these outsiders, and the team is subsequently employed to lead the UN inspectors on a guided tour of acceptable localities
- Local rich plantation owners seek to overthrow the governments control over the region by employing mercenaries to dissuade police from enforcing law in the area
- The team looking for one last payday actively courts tracking down *numero uno* on the C.I.As most wanted list - little do they know their prior indiscretions have raised the ire of another disgruntled group of mercenaries out for revenge

TRAINING & GM AWARDS

Generally at the climax of a plot *or* at the end of every game session, the Games Master should award additional Ranks for good gameplay. Players generally like to feel their character is steadily improving, by tying such improvements to good roleplaying it may help to keep your players motivated within the game, and not just taking the opportunity to catch up with friends. I highly recommend giving out specific improvements to a character that reflects a crucial action taken within the game – if a character saved team lives by an activity, reward it!

In addition, I like to give out 1 additional floating rank (*to go into any skill*) – a *GM Award*. It is generally given to the player who has come up with an outstanding plan, providing merriment, or who roleplayed effectively within their character.

If a skill is to be increased beyond a rank of *5*, one should require a running tally to be kept along the following lines (*see table below*). Due to the design of the game system characters quickly achieving ranks of 8 or 9 statistically present little to no challenge for the player.

Rank Improvement	Awarded Weeks
6th	02 awards
7th	04 awards
8th	08 awards
9th	16 awards
10th	32 awards

OTHER AIDS

Maps: If you base your campaign on a real location, it makes sense to have a map of it. However, you can even be more specific by downloading aerial shots from the web of 500 meter sections of most major cities. One such site is the British streetmap.co.uk site. Such aerial shots are useful for determining lines of sight, and basic dimensions of buildings. Frequently used locations can even be printed out and covered in plastic film, with the aid of white-board markers you can color code buildings just like in intelligence service operations.

Email: Gaming opportunities have improved with the use of email, not only do people manage to play complete roleplay games by turns on it, it can be useful for providing individual opportunities for character development. One can have everyday interactions with spouses, family and life events portrayed by email in between sessions – just how different would a special operations soldier react under combat pressure knowing his beloved is fighting for her life in hospital dying of cancer? This might seem redundant to some, but others might appreciate going a little deeper, and this way it guarantees that time isn't eaten up in game sessions.

Newspapers: If you are intending to run a game based on modern covert operations it is often useful to keep an eye on current political events that maybe harnessed in some way to give validity to your campaign world. The more you can successfully manipulate current events, the more plausible outlandish activities within the campaign will seem.

Internet: There have been many useful sites online that have added immeasurably to this resource, there are also a number of online military and espionage newsletters that you can subscribe to give you the latest information. Here is a list of some of the sites used in building this game engine…

SAS Rogues
http://www.sasrogues.co.uk/Home/home.html

Dudley Knox U.S Naval Library
http://library.nps.navy.mil/home/terrorism.htm

Israeli Special Forces Database
http://www.isayeret.com/main/guide.htm

F.A.S
http://www.fas.org/irp/index.html

Combat Online
http://www.combat-online.com/

The Spy Museum
http://www.spymuseum.org/do/

Terrorism Answers.com
http://www.terrorismanswers.com

U-Spy Store
http://www.uspystore.com

Spy Tech Agency
http://store.yahoo.com/spytechagency

Assassination
http://www.kimsoft/korea/cia-0.htm

Interrogation
http://www.kimsoft.com/2000/kubark.htm

Guerrilla Warfare
http://www/kimsoft.com/guerr-01.htm

Streetmap.co.uk
http://www.streetmap.co.uk

TerraServer USA Maps
http://terraserver-usa.com

15. USEFUL TABLES

CREATING AN NPC

Here are a series of tables that may be of some use in creating Player Characters & Non Player Characters

CHARACTER TRAITS

01 Addicted	26 Disloyal to Spouse	51 Jumpy	76 Proud
02 Aggressive	27 Easy Going	52 Kind	77 Quite
03 Amoral	28 Energetic	53 Lazy	78 Religious
04 Argumentative	29 Even Tempered	54 Liar	79 Reverent
05 Arrogant	30 Fanatic	55 Lusty	80 Rude
06 Blasé	31 Follower	56 Menacing	81 Scheming
07 Bookish	32 Foolish	57 Miserable	82 Selfish
08 Bore	33 Foppish	58 Moody	83 Silly
09 Brave	34 Forgiving	59 Neurotic	84 Skinflint
10 Capricious	35 Friendly	60 No Imagination	85 Slovenly
11 Careful	36 Frivolous	61 No Sense Of Humor	86 Spendthrift
12 Careless	37 Gambler	62 Nostalgic	87 Strong Opinions
13 Cheeky	38 Greedy	63 Not Very Observant	88 Stupid
14 Cheerful	39 Hardworking	64 Obsequious	89 Suspicious
15 Clever	40 Honest	65 Observant	90 Talkative
16 Close Mouthed	41 Honorable	66 Open Minded	91 Teetotaler
17 Collector	42 Hot Tempered	67 Optimist	92 Trusting
18 Compassionate	43 Humble	68 Overbearing	93 Uncivilized
19 Conceited	44 Impulsive	69 Overly Critical	94 Uncommitted
20 Confident	45 Individualistic	70 Passionate	95 Unforgiving
21 Conformist	46 Insensitive	71 Passive	96 Unfriendly
22 Cowardly	47 Irreligious	72 Perfectionist	97 Very Physical
23 Cruel	48 Irreverent	73 Pessimist	98 Violent
24 Curious	49 Jealous	74 Practical	99 Wastrel
25 Diplomatic	50 Jokester	75 Prejudiced	00 Well Mannered

APPEARANCE

01 Bad Breath
02 Bald
03 Bearded
04 Birthmark
05 Clean
06 Dirty and Unkempt
07 Distinctive Clothes
08 Distinctive Eyes
09 Distinctive Hair
10 Distinctive Jewelry
11 Distinctive Nose
12 Distinctive Scar
13 Distinctive Teeth
14 Fat
15 Florid
16 Freckled
17 Good Looking
18 Hairy
19 Hands Shake
20 Hard of Hearing
21 Jowled
22 Jug Eared
23 Light Build
24 Lisps
25 Missing Finger
26 Missing Tooth
27 Moustached
28 Nearsighted
29 Perfumed
30 Pockmarked
31 Potbellied
32 Puny
33 Short
34 Squints
35 Stocky
36 Stooped
37 Strong
38 Strong Body Odor
39 Stutters
40 Sweaty
41 Tall
42 Tanned
43 Tattoo
44 Thickset
45 Thin
46 Ugly
47 Walks with a Cane
48 Walks with a Limp
49 Wrinkled
50 Young Looking

MANNERISMS

01 Admires PC's Clothes
02 Arguing with Spouse
03 Blinks Rapidly
04 Is Very Busy
05 Chews on Toothpick
06 Clumsy
07 Constantly interrupts speech
08 Gives Racing Tips
09 Constantly winks
10 Doesn't like being touched
11 Fiddles with something
12 Flips a coin
13 Fusses with hair
14 Gets lost in thought
15 Hacking Cough
16 Hums
17 Monotone Voice
18 Mumbles
19 Nasal tone
20 Nervous Eye Twitch
21 Uses sweetheart, darling, sunshine
22 Shifts weight from foot to foot
23 Roll his 'r's'
24 Rubs Hands together
25 Runs Hand through hair
26 Scratches Head
27 Sighs Loudly
28 Sings
29 Slurps at Drink
30 Slurs Speech
31 Sniffles
32 Snorts when laughs
33 Speaks in Foreign Language
34 Speaks in Patronizing Manner
35 Speaks Softly
36 Speaks with an Accent
37 Spits often
38 Stares at attractive passers-by
39 Talks about health problems
40 Talk to herself
41 Talks very quickly
42 Talks very slowly
43 Drums fingers impatiently
44 Too drunk to talk
45 Tugs at beard
46 Twirls coin between fingers
47 Twists hair
48 Wheezy
49 Whines
50 Whistles

PROBABILITY TABLES

The following table gives the percentage chance of success for rolls in *theSpookEngine*. Numbers have been rounded and <1% represents less than one percent, whilst <<1% represents much, much less than one percent – a dash represent the result is impossible. Remember that the 2xd10 are the basic default dice.

Successes	0 Ranks (2 dice)	1 Rank (3 dice)	2 Ranks (4 dice)	3 Ranks (5 dice)	4 Ranks (6 dice)	5 Ranks (7 dice)	6 Ranks (8 dice)	7 Ranks (9 dice)	8 Ranks (10 dice)
botch	11%	10%	9%	7%	6%	5%	5%	4%	3%
0	31%	22%	16%	13%	10%	8%	7%	6%	5%
1+	58%	68%	75%	80%	83%	86%	89%	91%	92%
2+	26%	40%	51%	60%	67%	73%	77%	81%	84%
3+	7%	17%	28%	38%	47%	55%	61%	67%	72%
4+	1%	5%	12%	20%	28%	36%	44%	51%	57%
5+	-	1%	4%	8%	14%	21%	28%	35%	41%
6+	-	<1%	1%	3%	6%	10%	15%	21%	27%
7+	-	-	<1%	<1%	2%	4%	7%	11%	16%
8+	-	-	<1%	<1%	1%	2%	3%	5%	8%
9+	-	-	-	<1%	<1%	<1%	1%	2%	4%
10+	-	-	-	<<1%	<1%	<1%	<1%	1%	2%
11+	-	-	-	-	<<1%	<1%	<1%	<1%	1%
12+	-	-	-	-	<<1%	<<1%	<1%	<1%	<1%
13+	-	-	-	-	-	<<1%	<<1%	<1%	<1%
14+	-	-	-	-	-	<<1%	<<1%	<<1%	<1%
15+	-	-	-	-	-	-	<<1%	<<1%	<<1%
16+	-	-	-	-	-	-	<<1%	<<1%	<<1%
17+	-	-	-	-	-	-	-	<<1%	<<1%
18+	-	-	-	-	-	-	-	<<1%	<<1%
19+	-	-	-	-	-	-	-	-	<<1%
20+	-	-	-	-	-	-	-	-	<<1%

15. GLOSSARY

SPY A to Z

ACCESS: Possession of legitimate forms of security clearance to obtain classified information

ACCOMODATION ADDRESS: (see safe-house)

AERIAL ESPIONAGE: The use of all forms of aerial reconnaissance from manned or unmanned drone aircraft

AGENT: A person under the control of an intelligence agency, usually recruited by a member of the agency

AGENT IN PLACE: An agent established and working in a foreign hostile country

AGENT PROVOCATEUR: An agent seeking to incite and/or perform illegal acts to incriminate hostile parties, whether terrorist, or foreign agents

(BRIDGE) AGENT: A go-between agent who acts as a courier between a case officer and an agent under extenuating circumstances (as in limited access areas)

(CONFUSION) AGENT: An essentially dummy agent sent into the field to distract the hostile agency

(CO-OPTED) AGENT: An individual working for a foreign power willingly collecting information for an opposing intelligence agency

(COVERT) AGENT: An officer or agent performing covert activities

(DEEP COVER) AGENT: An agent in permanent, or well-prepared or highly advantageous cover

(DISCARDED) AGENT: An agent betrayed by his own intelligence agency, usually to protect a more important asset

(DOUBLE) AGENT: An agent who has turned against working for her local agency and working now in the interests of an opposing service. They may well be *turned* yet again

(NOTIONAL) AGENT: A fictionalized agent or mole, created for the purposes of misinformation

(REDOUBLED) AGENT: An agent who has turned and been discovered by their original agency, and is once again loyal

(TRIPLE) AGENT: An agent who serves three intelligence services, usually, not for very long…

(TURNED) AGENT: An agent who is *turned* into a double agent by force, threat or offer

(UNWITTING) AGENT: Someone who provides information without knowledge of their dealings with an intelligence agency

ALL SOURCE INTELLIGENCE: Intelligence gathered from all covert and open sourced materials and operations

ANGEL: Slang term for a member of an opposing intelligence service

ARTIST: (U.S) A trained forger working for the CIA's technical service

ASSESSMENT: An analysis of the validity of information or information source claims

ASSET: A intelligence resource, whether it be information or agent

ATTACHE: A foreign friendly civil servant, military personnel or agent assigned to liaison with allied forces, seeking to create greater understanding and sharing of information

AUDIO SURVEILLANCE: The use of audio equipment to eavesdrop on private conversations

BABYSITTER: Tradecraft slang for a bodyguard

BACKSTOPPING: A support activity to maintain cover for an agent – a phone line reserved for a 'former employer' enquiry's et al

BAGMAN: An agent who pays spies and bribes authorities

BANG & BURN: (U.S) A slang term for demolition and sabotage operations

BASIC INTELLIGENCE: The fundamental gathered facts about a country (social, economic, physical, cultural and political) established and validated

BIRDWATCHER: (UK) Slang for a spy

BIOGRAPHIC LEVERAGE: The use of secret background information about a person's history to blackmail them into providing intelligence and/or becoming an agent

BIOTERRORISM: The use of naturally occurring compounds, or the manipulation of chemicals to produce effective biological weapons

BLACK: As in 'black-bag-job', the slang term for illegal entry into an office or home to obtain files or other materials

BLACKLIST: An agency list of hostile collaborators, suspects, sympathizers or political dissidents who may threaten a countries security

BLACK-OPS: Clandestine or covert operations hopefully performed in such a way as to not give away aggressor's identity

BLACK PROPAGANDA: Information purporting to come from a different source which attempts to destabilize a foreign power

BLIND DATE: The organized formal meeting of an intelligence officer and her agent

BLOWBACK: Disinformation planted in foreign countries or media, which unfortunately filters back to the country of origin, causing scandal and embarrassment

BLOWN: A compromised operation, that may, or may not be detected by a hostile agency; yet which generally leads to the operation being withdrawn

BONA FIDES: The process of establishing an agent's true identity, affiliations or intentions

BRIEF ENCOUNTER: Any physical contact between an agent and case officer

BRUSH CONTACT/PASS: A covert exchange between an agent and the case officer (the exchange including such things including documents, cash or code word)

BUGGING: A term referring to all forms of eavesdropping (telephone tapping, parabolic mikes or electronic equipment)

BURN: A slang term for the deliberate sacrifice of an agent to a foreign agency, often for the strategic aim of protecting a more important agent in the field

C: Head of British Secret Intelligence Service (SIS) MI6 – Chief of the Secret Service

CALL OUT SIGNAL: An audio or electronic signal designed to trigger the contact of an agent to his/her case officer

CAMP PEARY (the FARM) (U.S): CIA Special Operations training school outside Williamsburg, Virginia

CAMP SWAMPY (U.S): CIAs secret domestic training base at Camp Peary

CAMP X: Canada's secret domestic training base

CANNON: A professional thief employed by an agency to recover information offered to an informant/agent

CARNIVORE (U.S): The FBI computer system to monitor email, internet and telecommunications lines within the United States

CASE: An intelligence operation from start to finish, or the record of those events

CASE OFFICER: An intelligence officer operating as either a controller or handler

CC&D: Camouflage, concealment and deception

CELL: The lowest rank within an espionage network, or a typical structure of a terror organization

CHATTER: Electronic Intercepts

CHICKEN FEED: Low-grade information supplied to double-agents to solicit trust and authenticity, to keep the opposition agency from suspecting they are being compromised

CIA (U.S): Central Intelligence Agency – Established 1947. The intelligence organization that seeks to extend U.S influence throughout the world

CIAink: Classified computer intranet housed at CIA HQ

CLANDESTINE (SERVICES): Covert operations unknown to the foreign agency. The Clandestine Services unit is the operational arm of the CIA for espionage operations

CLANSIG: Clandestine Signals Intelligence

CLASSIFIED: Information is classified to restrict the numbers of people with ready access to sensitive information, thus *Top Secret* information may well compromise a countries interests if it entered into the public domain. Higher grades of classification might require that information may only be kept in secure locations, may only be viewed *Eyes Only*, or the information may only be verbally related *Ears Only*

CLEAN: An agent who has never entered the field is known to be clean, that is, they have not taken part in prior operations, therefore they will generally not be recognized by tan opposition agency – at least on prior engagement grounds

CLOAK: A disguise or deception perpetrated by an agent to gain advantage in hostile areas of operation

COBBLER (RUS): A Russian slang term for a forger

CODES & CIPHERS: To create encrypted documents or computer files one needs to establish the fundamentals for breaking the code down, a cipher is the *public* or *private* key that has been decided upon prior by both parties as the method for reconstituting the encrypted information. Codes are an established series of numbers that set out a timetable of encryption, so the individual knows precisely what cipher to use

COLD APPROACH: An attempt to approach a foreign national for the purposes of making them an agent – without any prior indication of their desire to do so

COMMERCIAL ESPIONAGE: The attempt by a hostile country to promote their countries business interest by using their intelligence agencies to spy on foreign companies and governments

COMINT: The sub-category of SIGINT, which devotes itself to clandestine interception of foreign private communications

The COMPANY: The in-house name for the CIA

COMPROMISED: The asset, agent or operation that has been discovered and exposed

COMSEC: Communications Security methods of blocking or avoiding hostile SIGINT

CONCEALMENT DEVICE: A device used to conceal covert surveillance devices or documents

CONTROLLER: (Handler) A senior officer working under diplomatic cover or operation under deep cover, who controls the activities of agents (double-agents) in the field

COOKING THE BOOKS: The use of raw intelligence in a manner to promote a particular political stance or ideology

COUNTER ESPIONAGE: Measures taken to stop foreign agencies spying within one's own country, usually by measures of surveillance and interception of information

COUNTER-INTELLIGENCE: Activities undertaken to disrupt foreign agencies operations, taking active measures to stop their activities

COUNTER SURVEILLANCE: Actions undertaken undermine foreign surveillance operations

COUNTER TERRORISM: Proactive and responsive measures to eliminate the threats of terrorist activities within one's own country

COURIER: Is the agent responsible for the transportation of information, money or materials from agent to case officer. They are either informed of the contents or they can be used as CUT-OUTS.

COVCOM: Covert Communications

COVER: The false persona created for the purposes of spying, this may also be a measure of the level of concealment an individual has managed – deep cover being a total commitment to creating a 24/7 involvement

COVERT ACTION OPERATION: see Black-Ops

CRACKING: Illegal entry into a computer or computer network in order to do harm

CRITICAL INTELLIGENCE (U.S): The top level of classification for documents, which warns of imminent hostilities, which is immediately directed to the U.S Government highest echelons

CRYPTANALYSIS: The process of breaking down encrypted messages without access to the appropriate key

CRYPTOGRAPHY: The science of secret writing use in espionage and intelligence functions, whether it be by writing, electronic or audio means

CUT-OUTS: A person or process whereby information is passed between members of an organization, the person being completely unaware of the information

CYBERWAR: The general term for the process of using computers to spy or destroy opposing forces information capabilities

DAGGER (RUS): A sophisticated disguise first used by the Soviet Union

DANGLE: A person who approaches an intelligence agency with the intent to being a spy against her/his own country

DEAD DROP/DEAD LETTER DROP: The use of prearranged drop off points for the transfer of information or packages. This clandestine method means that the correspondents don't need to physically be in the same space to pass information

DEAD TELEPHONE: A signal or code pulsed down a telephone without need for speech

DEFECTOR: The foreign intelligence officer who wishes to abandon his former agency and work for the opposition agency. They can either be a *walk-in* defector who wishes to change their allegiances formerly, or they can be a *defector-in-place* who continues to work for the opposing services as a mole

DIRTY TRICKS: Operations undertaken to disrupt, confuse or damage opposing intelligence activities. From such things as spreading lies about the sex life or financial situation of foreign citizens, through to talking up the potential assassination of a foreign leader

DISINFORMATION: The process of creation and dissemination of false information to damage a foreign nation

D NOTICE: (U.K) A formal British censorship notice issued by the Home Secretary to stop the publication of an article which is deemed to compromise national security

DOCTOR (RUS): A slang Russian intelligence term for the police

DROP: The use of a clandestine location to drop material off for retrieval by an agent or case officer

DRY CLEAN: Actions undertaken to determine if one is under surveillance

EARS ONLY Information so highly classified that it can only be related in person orally in special facilities

ECHELON: The multinational surveillance network developed out of the UKUSA information sharing initiative, also including Australia, New Zealand and Canada; which uses satellite technologies to scan internet, email, telephone, fax for certain key words in the echelon dictionaries – and alerts the target country to any potential threats

ECONOMIC INTELLIGENCE: The use of intelligence gathering and espionage to destabilise a foreign powers economy

ELECTRONIC WARFARE: The general term to detect, locate and reduce or exploit a foreign powers use of the electromagnetic spectrum

- Electro-Optical Intelligence (Electro-OPINT) intelligence gathered from the ultraviolet to the infrared spectrum
- Electronic Intelligence (ELINT) intelligence gathered from electronic devices such as radar and machinery (does not including atomic or radioactive emissions)
- Electronic Counter Measures (ECCM) measures undertaken to repulse or disguise electronic or electro-optical emissions

ELICITATION: The ability to gather information from a conversation with a group or individual without divulging the intent of investigation

EMISSION CONTROL (EMCON) & SECURITY: The reduction or total avoidance of radio and radar transmissions to stop hostile forces from intercepting

ESCAPE & EVASION: Intelligence and military techniques taught to avoid capture and evading one's captors

ESPIONAGE: The basic activity of spying on a foreign country

ESTABLISHED SOURCE: A long-term reliable source, which requires little in the way of verifying

EXECUTIVE ACTION: Intelligence term for a sanctioned assassination attempt

EXFILTRATE (OPERATION): A clandestine rescue of a defector, refugee or agent (+ family) from a hostile zone

EXPLOITATION: The systematic attempt to produce the maximum amount of information out of an agent or source. Often to the detriment of the individual

EYES ONLY: Security classification of documents of high importance that should not be orally discussed, except in certain high security level environs

FALSE FLAG: The act of pretending to be a representative of a competing intelligence organization

FBI (U.S): The Federal Bureau of Investigations (U.S internal security agency)

FENCE (RUS): A Russian term for border between countries, or more generally, an individual who buys and sells stolen goods

FERRET: Electronic intelligence platform, like an aircraft or satellite
FIELD (U.K): British term for being in foreign territory, as in, I'm currently *in the field*

The FIRM: The popular nickname for the CIA (also the Company)

FIX (U.S): CIA term for compromising, blackmailing or conning an individual

FLAPS & SEALS: The intelligence activity of creating surreptitious opening and closing in envelopes

FLASH: Highest precedence in CIA cable communications

FLOATER: A freelance agent who is used occasionally or once, usually someone like a waiter, taxi-driver

FOOTS: Members of a surveillance team who move about the target on foot, or are dropped at locations from passing surveillance cars

FORGERS BRIDGE: A technique to brace together both hands of a forger to steady the flow of handwriting for accuracy

FRENCH OPENING: A method of surreptitious opening of letters, by slitting one end and resealing

FRIENDS (U.K): A term for the historically close ties between MI6 and the British establishment

FRONT: A business front set-up in foreign territories to mask an undercover operation

FUMIGATING: A slang term for checking for surveillance devices within a building

FUSION: Process of examining all intelligence and deriving an accurate overall assessment of the situation

GAMBIT: A specific disguise technique developed by the CIA and Hollywood make-up artists which make it possible for realistic ethnic changes

GAMEKEEPER (U.K): British slang term for an agent controller or handler

GARDENING (U.K): An operation designed to force the opposition to send a coded message to their superiors, with the express purpose of breaking the code

GCHQ (U.K): Government Communications Headquarters is the British agency, which seeks to intercept communications internally and externally

GHOUL: An agent who searches obituaries and graveyards for names of the deceased for use by agents

The GREAT GAME: A term originally coined by Rudyard Kipling for the intrigues associated with British rule of India, now more prominently associated with the Cold War and its rules of engagement

GREY MAIL: The threat in a trial by defendant to expose various members of the intelligence agency

HANDLER: The case officer responsible for the activities of agents and operations

HF DF (Huff Duff): High Frequency-Direction Finding is the use of triangulation of radio signals to pinpoint the source of a transmission

HONEYTRAP: An operation, which seeks to lure a target via sexual promises

HOSPITAL (RUS): A slang Russian term for a prison

HOSTILE: The opposition agency, which poses an immediate threat

HUGGER-MUGGER (U.K): An operation reliant upon maximum secrecy or stealth, often also used to describe an errant operation

HUMINT: Human Source Intelligence is any information derived from agent activity or informants

ILLEGAL: An intelligence officer working in a foreign realm in disguise as a private person, often using false identification – expressly without diplomatic immunity

IMINT: Imagery Intelligence meaning all imaging technologies to generate images, including satellite imagery, generally replacing the use of PHOINT (Photographic Intelligence)

IMMEDIATE: The 2nd highest precedent in CIA cable communications

IMPERSONAL COMMUNICATIONS: Secret methods of transferring messages from agent to case officer, requiring no physical contact

INDICATION & WARNING: Intelligence operations expressly designed to help determine any immediate threats to national security

INDUSTRIAL ESPIONAGE: The use of agents to undermine the production capabilities of an international competitor

INFILTRATION: The covert movement of an agent or team into a foreign secure zone

INNOCENT POSTCARD: A postcard set with an innocuous message sent to an address in a neutral country to verify the continued security of an undercover operative

INTELLIGENCE: The product of collecting, processing, evaluating and analysing all forms of surveillance

INTELLIGENE APPRECIATION (U.K): (see Intelligence Estimate)

INTELLIGENCE CYCLE: In any intelligence operation, there are a number of definable steps including; planning and direction, collection, processing, production and analysis and dissemination or distribution

INTELLIGENCE ESTIMATE: The appraisal of all available intelligence in regards to a particular issue, or a potential operation

INTELLIGENCE OFFICER: A salaried member of an established intelligence service

INTELLIGENCE PRODUCER: The intelligence officer responsible for developing all forms of documentation in the production stage of operations

INTELLIGENCE REQUIREMENT: The general area or specific area, which has been identified as an area of deployment for the intelligence agency

INTERCEPTION OF ORAL COMMUNICATIONS: Spy parlance for bugging

INTERDEPARTMENTAL INTELLIGENCE: The collation of information from various sources for the benefit of all agencies

JACK IN THE BOX: A dummy inserted into a car to deceive surveillance activities

KNUCKLE DRAGGERS (U.S): Slang term developed for the CIA branch of Special Operations, purportedly by other arms of the service

LEGAL: An intelligence agent operating in a country in a official position, like a cultural attaché or working in an embassy

LEGEND: The development of a complete, rounded cover story

LINK ENCRYPTION: The use of online applications to encrypt communications

LISTENING POST: Any audio surveillance site developed to intercept information, from an OP unit up to a permanent monitoring site like Menwith Hill

L PILL: A *lethal* cyanide capsule

MAIL COVER: The request from an intelligence agency to the appropriate mail authorities to examine the outside of mail and packages for the purposes of intelligence gathering

MAIL DROP: The delivery of mail to a specified location

MAJOR DOCS: A slang term for the major documents developed for the purposes of an alias

MASINT: Measurement and Signature Intelligence (a specific TECHINT devoted to measurement of angle and special wavelength, time dependence of modulating signals and hydro-magnetic data. Can also include measurement of air and water samples)

MATINT: Material Intelligence seeks to gain knowledge by looking at the methods of mechanical engineering and materials engineering; in the development of specialist kinds of materials for say, weapons and aircraft design

MEASLES: A Cold War slang term for an efficient assassination, which the opposition might euphemistically put down to a bad case of *measles*

MEDICAL INTELLIGENCE: The use of medical tests devoted to informing about the relative health of leading oppositional forces

MI5: The original cover name for the British Security Service, responsible for internal security

MI6: The military cover name for the British Secret Intelligence Service, responsible for British intelligence gathering abroad

MICE: The abbreviation of the four motivations why people become spies, they being; Money, Ideology, Compromised or Ego

MICRODOT: The Cold War use of photographic reduction to hide secret information in documents or photos

MINARET (U.S): The highly classified programme of the NSA to incept civilian communications from foreign sources

MISSION: A task to be undertaken by an agent or officer, which is clearly defined in reason, purpose and action

MOLE: Is an agent who is ostensibly working on behalf of a foreign agency for the purposes of gathering information from the inside

MOSCOW RULES: A particular set of tradecraft rules developed and designed for operations in hostile environments

MUSIC BOX (RUS): A Russian slang term for a hidden radio set

MUSICIAN (RUS): A Russian term for a radio operator

NAKED: The deployment of an agent in an area where they have no immediate assistance to aid them

NEED TO KNOW: The operational basis whereby security is maintained by restricting the flow of information on a *need to know* basis

NEGATIVE INTELLIGENCE: Intelligence gathered which is confirmed to be from a compromised or hostile source

NETWORK: A group of undercover agents or illegals working in a foreign environment through the central control of a handler

NEWS: Usually, *Bad News*

NIGHTCRAWLER: An *agent talent* spotter who frequents night-clubs and bars looking to compromise any errant government employees or military personnel

NSA (U.S): National Security Agency is the SIGINT agency of the United States

NUGGET (U.K): The bait of money, asylum or sexual favours used to lure a foreign national into service

NURSEMAID (RUS): A slang term for a security official who travels with delegations to stop participants defecting

OPEN SOURCE or OSINT: Open Source Intelligence, which is derived from readily available sources; such as newspapers, census or publications

OPERATIONAL INTELLIGENCE or OPINTEL: Intelligence gathered specifically for the purposes of operations within a set region

OPERATIVE: An intelligence officer or agent operating in the field

OPSEC: Operations Security, the means by which operational integrity are maintained at all times

ORCHESTRA (RUS): The Russian term for the development of long term sleeper agents in hostile areas

OVERT INTELLIGENCE: The gathering of intelligence for public information sources

OWVL: One-way-voice-link, a short-wave radio transmission to an operative

PADDING: The additional words included at the beginning and end of a transmitted message to scramble any potential decrypting activities

PAROLES: Passwords to identify agents to each other

PATTERN: The observed daily routines of a suspect under surveillance

PAVEMENT ARTIST: Slang term for any experience street surveillance expert

PDB (U.S): President's Daily Brief, giving an overview of potential threats to national security and external conflicts

PERSONAL MEETING: A clandestine meeting between two operatives

PHOTINT: Photographic Intelligence, is now more commonly known under the umbrella of IMINT (image intelligence), as photographs are now usually digital in nature

PIPELINER: An intelligence officer who is currently being trained to deal with specific operational requirements of a region

PIANIST: Western term for clandestine radio operator

PIANO: Western term for clandestine radio

PLAIN TEXT: The original message before encryption

PLAUSIBLE DENIAL (U.S): This term is derived from the CIA response to the exposure of atrocities committed by the agency in the 1960s and 70s, which subsequently came to light in the Congressional Church hearings. It consists of a range of measures to ensure superiors within the CIA and politicians aren't held responsible for black-ops operations of a sensitive nature. The range of measures including; avoidance of discussion amongst senior ranks of the specifics of operations, the development of new euphemism to avoid direct discussions, and the avoidance of creating records of conversations or other documentation

PLAY BACK: The act of providing false information to the enemy whilst receiving accurate information whilst impersonation a friendly spy

PLUMBING: The activity of preparing a building for an operation by placing an assortment of bugs and surveillance devices (plumbers)

PNG: Person Non Grata, the diplomatic expulsion of a diplomat, for immoral acts or being a spy

POACHER (U.K): A term for a foreign spy currently lurking in an operational area

POCKET LITTER: The items within a spy's pocket (receipts, coins, theater tickets etc) that add authenticity to his or her identity

POLITICAL INTELLIGENCE: Any intelligence information that may shed light upon the political scene, and consequences, of a foreign power

POSITIVE VETTING (U.K): The British Government comprehensive security check performed, when someone is applying for sensitive government posts or under MI5 investigation

PROBER: An operative sent to check out the border controls ahead of exfiltration operation

PRODUCT: The final result of an intelligence operation or espionage

PROFILE: A complete listing of a target's attributes

PROPRIETARY COMPANY (U.S): A CIA term for a commercial asset established for an operational front

PROVOCATION: An activity or procedure undertaken to expose surveillance operations

Q CLEARANCE (U.S): The security clearance needed to access U.S restricted nuclear data or weapon material

RADINT: Radar Intelligence, intelligence gained from the use of radar installations, widely now subsumed under IMINT

RAVEN: A male operative used to seduce either male or female targets

RECONNAISSANCE: Operations with the intent to gain knowledge of a site or target for later potential engagement

REPRO: Reproduction, making a false document

RESIDENT (RUS): The name of a KGB/SVR chief of a station in a foreign location

RESIDENTURA: The subsequent station, which is likely to be found in their embassy

ROLL-OUT: A technique of surreptitiously rolling out the contents of a letter through the use of pen or a knitting needle

ROLLED UP: The term for when an operation goes awry or an agent is compromised

RPV: Remotely Piloted Vehicle, drones or UAV units employed in the field to gather IMINT cost effectively

SAFE HOUSE: A secure house considered safe for operative use as a base of operations, and even to perform interrogations

SANCTIFICATION: Blackmail specifically performed to grant political favour

SANCTION: The term for intelligence agency approval for the killing of a target, for revenge or strategic countermeasures

SANITISE: To delete specific information from reports to reflect a particular bias

SCALP HUNTERS (U.K): British slang term for intelligence officers who specialise in detecting genuine defectors from plants

SCIENTIFIC INTELLIGENCE: The specific intelligence gathering operations devoted to science and technology of a foreign country, i.e weapons development

SCIF: Sensitive Compartmented Information Facility

SDR: Surveillance Detection Run, a particular course of action designed to expose counter-surveillance measures, hopefully without alerting to opposition to one's purpose

SECRET WRITING: The tradecraft devoted to the sending and decoding of secret texts, like microdots or invisible inks

SETTING UP: The framing or entrapment of an individual by covert means

SHEEP DIPPING (U.S): A term for camouflaging the true identity of equipment or individuals, usually military assets

SHOE (RUS): Russian Intelligence slang word for a passport

SHOE MAKER (RUS): Someone who makes false passports

SHOPPED (U.K): British term for an individual being deliberately exposed

SHOPWORN GOODS: Old intelligence information that has done the rounds

SIGINT: Signals Intelligence, all manner of intercepted communications including radio transmissions, telecommunications transmissions

SIGNAL SITE: A fixed location known by both parties where a distinctive mark can be left to signify some particular meaning

SIS (U.K): Secret (Special) Intelligence Service MI6

SITREP: Situation Report, a report regularly sent to update an officers activities or a special crisis report

SLEEPER: A foreign agent deep undercover in opposition territories not activity spying, but awaiting set orders to activate

SOAP: The nickname for the so-called truth drug, Sodium Pentathol

SOFT TARGET: Human Targets

SOURCE: Anyone who relays information to an agency without knowledge of its usage

SPECIAL BRANCH (U.K): The special investigations arm of the British Police Force

SPECIAL TASKS (RUS): Russian euphemism for assassinations, kidnapping or sabotage operations

SPONSOR: The intelligence term for the agency sponsoring any particular operation

SPOOK: General term for a spy

SPY: Any member of an intelligence agency actively engaged

SPY SWAP: The formal exchange of spies between two hostile countries

STAFF AGENT (U.S): A CIA staff officer without access to secure faculties or classified communications

STAGE MANAGEMENT: The basic principles of orchestrating operations to account for any potential problems and creating contingencies, plus accounting for any areas where the operation might be compromised

STATION: A CIA base for field operations, usually outside the U.S

STEPPED-ON: Deliberated interference to radio traffic

STERILISE: To remove any information from operational outcomes, which may compromise the sponsoring service

STRINGER: A low-level agent who occasionally passes on information, such as a taxi driver

STROLLER: An agent on foot operating a walkie-talkie or wired up for street surveillance activities

SUCKING DRY (RUS): A term for the deliberated long debriefing of an agent

SURREPTITIOUS ENTRY UNIT (U.S): A unit of CIA Technical Service devoted to opening locks and gaining entry into secure faculties

SVR (RUS): Sluzhba Vneshney Raszvedki Rossii or Russian Intelligence Service

SWEEPER: An electronic technician who sweeps offices and facilities for bugs

SWALLOW (RUS): A Russian term for a female agent in a sex entrapment operation

The TAKE: Slang for the information gathered by espionage

TACTICAL INTELLIGENCE: The specific intelligence used in the planning of a tactical operation

TALENT SPOTTER: An intelligence officer specially trained to recruit new agents through honest or nefarious means

TARGET: The individual, facility or agency the operation is directed towards

TARGET OF OPPORTUNITY: A target who may come to light during an unrelated operation

TAXI (U.K): A slang term for a homosexual member of an entrapment operation, also variously known as jacksie, ladies, sisters, or a reversal of swallows

TECHINT: Technical Intelligence, the umbrella term for IMINT, SIGINT and MASINT

TELEPHONE TAPPING: The deployment of covert surveillance technologies to overhear private telecommunications transfers

TELINT: Telemetry Intelligence, (part of MASINT) such as intercepts from foreign missile tests

TEMPEST: Transcient Electro-Magnetic Pulse Emanation Standard, electrical equipment regularly emit electro magnetic pulses, the science of van Eck monitoring seek to identify equipment on foreign soil by these emissions

TIMED DROP: A type of drop that is retrieved if not picked up in a set timeframe

TINKERBELL:

TOSSES: A type of drop used by throwing an object from a speeding vehicle

TRADECRAFT: Various professional spy disciplines developed to improve operational efficiencies, such as forgery

TRAFFIC ANALYSIS: A form of SIGINT, which analyses the volume and types of communications, and looks for any emerging patterns that may provide information

UAV: Unmanned Aerial Vehicle, a drone aircraft, land or sea vehicle used for reconnaissance purposes

UKUSA: An agreement signed in 1947 formalizing a degree of co-operation between US and UK SIGINT

UNCLE: Headquarters of any espionage service

WALK IN: A defector who walks into a hostile country's installation or embassy wanting political asylum

WALKING THE CAT (U.S): The systematic retracing of the steps of a *blown* agent back to the origin of operation to see if they can identify the point at which they were compromised

WATCHCON: Watch Condition, a military I&W rating system and ranking of world hotspots

WATCHERS (U.K): A member of MI5s A4 surveillance section

WATCH LIST: A list of persons considered to be of interest to an intelligence agency

WET AFFAIR (RUS): An operation that will involve killings

WET SQUAD (RUS): A Russian assassination team

WHITE: An unclassified or acknowledged classified project, or an agent who has no field experience – therefore unlikely to be compromised

WHITE MEAT: A derogatory target used by some Islamic terrorists to describe Western (but mainly U.S) civilian targets

WINDOW DRESSING: The accumulation of facts in a cover story not essential, but give the appearance of being a believable cover story

ZOO: A Western intelligence term for a police station

MILITARY A to Z

A

AAA - Anti Aircraft Artillery
AFV – Armored Fighting Vehicles meaning any vehicle which is armored and armed
AGM - Air Ground Missile
AO - Area of Operation
APC – Armored Personnel Carrier
ARM – Anti-Radiation Missile seek out and in on radar emissions
Armored – The basic definition given to vehicles with protection for passengers and crew
ATGM - Anti Tank Guided Missile
APC - Armored Personal Carrier used primarily for transporting troops
ATV - All Terrain Vehicles
AWACS – An Airborne Warning And Control System

B

Badged – An SAS term for someone who has passed selection training, and got the fabled winged dagger
Basha – An SAS term for a shelter, usually temporary
BDU – Battle Dress Uniforms
Bergan – An SAS term for a waterproof backpack or rucksack
Big Four – A standard description of the four pieces of information captured soldiers are allow to give under extreme interrogation – name, rank, date of birth and number
Bird Strike – A term for the potentially lethal occurrence of a bird hitting a vital part of a plane
Bivi-Bag – A British military slang term for a waterproof sack
Blood Chit – Some special-forces issue pieces of paper to soldiers behind enemy lines, in case of the mission being compromised and the soldier needs to obtain local help – the document can be redeemed at the nearest embassy (of the special forces country) for a sum of money
Blood Money – Most special-forces soldiers are issued with gold coins when working behind enemy lines, to buy their freedom or get aid if the operation goes wrong
Buddy-Buddy System – An SAS term that symbolizes the need for some units to work closely in two-man teams
BUDS – Basic Underwater Demolitions Seal training, US Navy Seals course

C

Caliber – Each firearm uses varying widths of bullets for greater damage or flight time
Callsign – A basic designation of a unit or individual for radio communications
Casevac – Abbreviation for Casualty Evacuation, a solider seriously in need of medical care
CBR – Chemical, Biological Radiological agents
Centerfield – A US Navy Seals term for a technique of extraction from a firefight
CFV – Cavalry Fighting vehicle used primarily for scouting, essentially armored cars
Chobman – A strong composite tank armor to effectively negate HEAT missiles
CO - Commanding Officer
Contact – A term to denote contact with the enemy, usually a gunfight
Contact Drill – Training for contact situations
Control Risks – A term for the measurement of risk associated with an operation
Cross Training – The term to denote most special ops delving into more training than their specialization
CQB - Close Quarters Battle
CT - Counter Terror
CTR – Close Target Recce
CSAR - Combat Search And Rescue

D

Delta Force – The name given to the US 1st Special Forces Operation Division
Double Tap – The name given to the firing of two bullets in succession favored by special-forces

E

EOD - Explosive Ordnance Disposal
Escape and Evasion – A group of skills to avoid capture in hostile environments
EW – Electronic Warfare
Eyeball – A British Surveillance and Military term for having visual on the target

F

FAV – Fast Attack Vehicle
FASCAM – Field Artillery Scatterable Minefield consisting of antitank or anti-personnel mines fired quickly from artillery rounds to halt enemy movement
FFP - Final Firing Position (usually refers to snipers work)
First Light – A military term for dawn, when the enemy is likely to start being active
Flashbang – A type of grenade that produces a non-lethal flash of light and sound to disorientate
FMS - Foreign Military Support
FLIR - Forward Looking Infrared which analyses heat radiation data
Frame Charge – A type of entry explosive made of plastic explosive, molded to fit door, window or wall

G

Gillie Suit – A netted camouflage suit designed to stuff with local flora to blend in with surroundings
GPMG - General Purpose Machine Gun
GPS - Global Positioning System
Green Machine – A nickname given to the regular British Army
GSC9 – The acronym for the elite German counter-terrorist unit the Grenzshutzgruppe 9

H

HALO – High Altitude Low Opening Parachuting
HAHO – High Altitude High Opening Parachuting
Hatton Round – A solid slug used in shotguns, primarily for blowing hinges off doors
Hearts and Minds – A term for psychological operations
HEAT - High Explosive Anti Tank (usually refers to anti tanks missiles)
Heavy Forces – The combined usage of tanks, mechanized infantry and self-propelled artillery
Hide – A British term for a location for a cache of weapons or Observation Post

I

IAF - Israeli Air Force.
IFV – Infantry Fighting Vehicles is a vehicle designed for both transport and firepower
ICM – Improved Conventional Munitions seek to create artillery munitions which fracture in mid-air to allow for the release of bomblets (to scatter over a wider area and cause more devastation)
IDF - Israeli Defense Force
Indirect Fire – A form of combat where the soldier cannot see the enemy, usually long-range artillery were scout reports provide the basis of targetting
IR - Infra Red

L

LBH - Load Bearing Harness
LBV - Load Bearing Vest
LIC - Low Intensity Conflict
LMG - Light Machine Gun
LO – Liaison Officer
LRRP - Long Range Reconnaissance Patrol
LS/LZ – Abbreviation of Landing Sight or Landing Zone
LSV – Light Strike Vehicles

M

M4 - the carbine version of the M16A2
MAGAV - Israeli Border Guard
MATKAL – Israeli General Staff (the IDF High Command)
MBT – Main Battle Tank is a frontline tank for intense firefights
Meat Eaters – A US term for top disciplined soldiers
Mechanized – The type of infantry that rides into battle in APCs or IFVs
MLRS – Multiple Launch Rocket System
MOE – A British acronym for Methods of Entry
MOS – Military Occupational Specialty is the main vocation of a soldier ie tank crewman, radar technician
Mossad - Israel foreign intelligence gathering organization
MRE – Meal Ready to Eat, a type of military ration, with a pad on the side to add water to heat
MSR – Main Supply Route
Motorized – the definition of soldiers who ride into battle aboard trucks or unarmored vehicles

N

NBC - Nuclear Biological Chemical
NCO - Non Commissioned Officer
NVD - Night Vision Device
NVG - Night Vision Goggles

O

OP – Observation Post

P

P for Plenty – A term used by the British SAS to describe erring on the side of caution when using explosives
PDW - Personal Defense Weapon
Pinged – A phrase to denote spotting the enemy or identifying objective
Platform – A navy term for any of its vessels (whether ship or submarine)
Prayers – A British slang term for the operation briefing in the morning
Psychological Warfare – The term denotes the propaganda activities carried out by militants

Q

QRF – Quick Reaction Force

R

RHIB – Ridged Hulled Inflatable Boat
RPG – A type of rocket propelled grenade
Rules of Engagement – A standard set of SOPs observed by most military organizations to not start unwanted conflicts
R&R – Rest and recuperation
RV – Abbreviation of Rendezvous Point

S

SAM - Surface Air Missile
SAR - Search And Rescue
SDV – Swimmer Delivery Vehicle
Seals – The US Navy's Navy Seals Unit
SF - Special Forces
Shake Out – A British term for a rehearsal of an operation, to *shake out* the faults
Shoot To Kill – An erroneous phrase attributed to SAS activities in Northern Ireland
Sitrep – An abbreviation of Situation Report
SOP – Standard Operating Procedures
SMG - Sub Machine Gun
SSM – Surface to Surface Missile
SWAT - Special Weapons And Tactics
SWS - Sniper Weapons System

T

Tailend Charlie – A military term for the man patrolling the rear
TA – Territorial Army
T&E - Testing & Evaluation

U

UAV - Unmanaged Aerial Vehicles

W
Washup – An alternate word for debrief
White Out – A term for a zero-visibility situation because of cloud or blizzard

X

XO - Executive Officer (second in command)

Z

Zulu Time – The widely used term for Greenwich Mean Time GMT – to organize worldwide activities

17. SAMPLE AGENCY MI5

Mi5 – The Security Service

Type of Service: Internal Security Agency
Field of Operations: United Kingdom & Northern Ireland
Arrest Powers: None
Executive Powers: No Firearms/Wiretapping (authorization through Home Office)
Annual Funds: £200 million pounds (approximate figure)
Number of Staff: 2,400 individuals (not including agents)
Headquarters: Thames House, situated at Millbank London
Founded: **1st of October 1909**
Current Director General: Eliza Manningham Buller
Reports To: Home Secretary *David Blunkett* + Joint Intelligence Committee
Technology Availability: Above Average
MI5 Public Assistance Phoneline: 020 7 930 9000

Operational Remit: *The Defense of the Realm against terrorism, espionage and subversion. Recently, since the introduction of the* Security Service Act 1996*, its role has been expanded into assisting in organized crime, supporting law enforcement activities and assisting in serious crime investigations. It also has* primacy *in intelligence operations in Northern Ireland*

A Brief History:

- 1909 March Founded after Prime Minister Asquith instructed the Committee of Imperial Defense to consider the dangers of German espionage on British Ports
- 1909 October Creation of Secret Service Bureau under auspices of Military Operations Directorate
- 1910 Control moved to Home Section under control of Captain Vernon Kell (also known as K)
- 1914 Becomes part of Directorate of Military Intelligence MO5(G) and changes of function to include vetting, security and oversee counter-espionage in Europe
- 1917 After Bolshevik Coup D'état communism subversion becomes major threat
- 1926 During Trade Union General Strike, subversion becomes a pressing issue
- 1940 Captain Kell resigns after hysteria related to undiscovered German spies furore and registry records are destroyed in a major fire
- 1942 Sir David Petrie is placed under control as first Director General, funds are forthcoming to expand operations
- 1945 Records show some 200 German spies were discovered during the war years and d*ouble-crossed* (became double-agents)
- 1948 Vetting system strengthened after *Cambridge Spies* wartime activities
- 1952 Prime Minister, Winston Churchill hands responsibility of the service to the Home Secretary (Home Office - Whitehall) + service becomes a civilian organization (previously under military)
- 1960s-70s Service name blackened by high profile scandals like the Profumo Affair, and allegations that Labour Prime Minister Harold Wilson was actively undermined by some agents
- 1980 Iranian Embassy tests the ability of the service to act in concertina with other services
- 1984 Bombing of Conservative Conference in Brighton serves to highlight the disparities in the direction of dealing with the Northern Ireland problem (MI6 + MI5 fighting for primacy in province + lack of communication exposed)
- 1989 Scandal involving prominent MI5 director John Deverell after breaches of law enforcement agreements between Britain and Germany in operations to establish Irish informers
- 1989 After persistent accusations of the lack of secrecy maintained within the service a Security Commission inquiry takes place, Sir Anthony Duff is installed as new Director General and Security Service Act 1989 outlines new procedures and defines the legal status of the service
- 1991 Irish mortar attacks on Downing Street

- 1992 The Security Service is given primacy in Northern Ireland intelligence gathering, it is seen as compensation for the end of the Cold War, and the Royal Ulster Special Branch feels aggrieved after 110 years experience in dealing with the threat
- 1994 Deverell and 25 other intelligence personnel (including division heads) and 4 RAF crew on the way to a conference via Chinook helicopter at Fort George, Scotland – most major senior staff in Northern Ireland said to have been killed
- 1994 Director General, Stella Rimington disbands G7 responsible for Islamic Terrorists believing the threat over – despite 1988 Lockerbie bombing over Scotland
- 1999 Despite some arrests in Northern Ireland and the end of hostilities in the province, belief is the service is changing far too slowly to deal with immerging threats elsewhere + 50% of operatives are now age 30 years old or less
- 2001 Islamic terrorists actions in America destroy the World Trade Center in New York and parts of the Pentagon via hijack planes (ushers in a new age of terror)
- 2004 Great efforts are being undertaken to expand the base of staff to deal with the Al-Qa'ida threat

STRUCTURE & ORGANIZATION

A Branch Surveillance
A1 Operations including…
A1A Bugging and Break-Ins
A1B Obtaining personal data from DHSS, Inland Revenue and Banks
A1C Running of 'safe houses'
A1D Expert locksmiths, safe crackers and carpenters
A1E Electronic Monitoring (provides tapes to A2A)
A2 Technical Back-Up (surveillance devices)
A2A Transcription Tapes
A2B Specialist Photographs and electronic experts (liaison with GCHQ)
A4 Direct Surveillance (aka the Watchers) + vehicles
A5 Scientific Research
B Branch Personnel
B1 Recruitment
B2 Personnel Management
B3 General Management Services
B5 Finance

C Branch Protective Security
C1 Security in Whitehall
C2 Vetting Government Contractors
C3 Vetting Civilians and Ministers
C4 Security Against Terrorist Attacks

D Branch Counter Espionage, Organized Crime, Subversion and Arms Proliferation (no breakdown available)

F Branch Domestic Surveillance
F1 Communist Party (CPGB)
F2 Trade Unions
F2N Trade Union Leaders
F2R Media, Education, MPs and entertainers
F3 Non-Irish Terrorism
F4 Agents in CPGB, Trade Unions and Journalism
F5 Irish Terrorism
F6 Agents in Radical Groups and Terrorist Organizations
F7 Surveillance of Political Lobby Groups (Anarchists, Extreme Feminists, Green Groups 'etc')

G Branch International Terrorism (no breakdown available)

H Branch Strategic Planning, Information Technology and Finance (no breakdown available)

K Branch Counter-Intelligence
K1 Potential Espionage In Government Departments
K2 Monitoring Russian Military Intel
K3 Recruitment of Russian Agents
K4 Surveillance of Russian Diplomats
K5 Recruitment of Eastern European and Chinese Agents
K6 Recruitment of other hostile agents in UK
K7 Investigation of penetration of UK security and intelligence agencies
K8 Non-Russian Counter-Intelligence

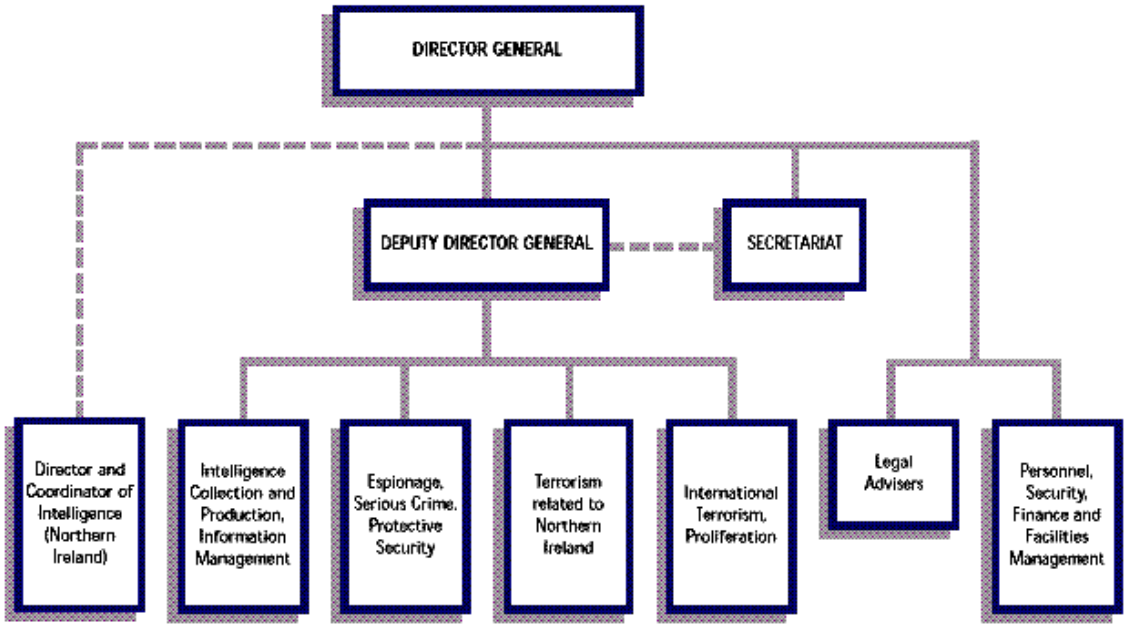
Now Grouped Under…
KX Investigative Work (including K1, K2 & K3)
KY Operations (including K4, K5, K6, K7 & K8)

S Branch Training & Computer Systems
S1 Runs Joint Computer Bureau (linked to agencies like MI6)
S2 Registry of Files
S3 Training
S4 Supplies and Travel Arrangements

Thames House Headquarters

T Branch Anti-Terrorism
T1 Irish Terrorism
T2 Non-Irish Terrorism

General Intelligence Group (GI) this section is comprised of 300-400 officers, which can be readily assigned to other sections in times of need



The service operates under the statutory authority of the Home Secretary, although it does not form a part of Home office operations. The fundamental basis for the operations of the security service, being both covert and invasive into the lives of some citizens ensures there is continued tension between its operations and public (and government) goodwill.

The 1989 Security Service Act seeks to apply some accountability to its operations. The Director General is appointed in consultation between the Home Secretary and the Prime Minister, the Director is required to submit a report annually. The Director General is also statutorily responsible for all aspects of its operations and efficiency.

The Act provides for an independent tribunal, with support from a Commissioner (a senior judge) to investigate public complaints about the service and its operations. The Commissioner is also responsible for reviewing the issue of Secretary of State Property Warrants under the Intelligence Services Act 1994

The Interception of Communications Act 1985 provides for a tribunal, supported by the Commissioner (a senior judge) to review the issuing of interception warrants by the Secretary of State (Home Secretary).

The service's performance, plans and priorities are scrutinized by a senior Whitehall committee known as Security Service Priorities and Performance or SO(SSPP), which reports to Cabinet Ministers

The Director General has a Deputy who is responsible for overseeing intelligence operations. There are five different branches, headed by a Director – three deal with intelligence investigations and advising protective measures to counter threats, whilst two others are responsible for intelligence collection, production and information management; plus personnel, security finance and facilities management. There is also a department devoted to Legal Advisers. There is also a relatively new department devoted to Northern Ireland intelligence, who reports to both the Director General and Secretary of State for Northern Ireland.

The Director General, Deputy Director General, the Directors and Legal Advisers all regularly meet as the Management Board of the Service to discuss strategic planning, policy and priorities. The service currently employs around 2,400 people; most of them are based in the headquarters at Thames House on the embankment, London.

The Home Secretary receives briefings on threats to national security from the Director General's office daily. The briefings are also made available to the Prime Minister's Office and MPs. The Home Secretary personally authorizes all warrants allowing for the interception of letters, phonecalls and other media, or to interfere with property.

The Intelligence and Security Committee established under the auspices of the Intelligence Services Act 1994 comprises of nine parliamentarians (drawn from both the House of Commons + House of Lords). The committee is appointed by the Prime Minister and makes an annual report (who will submit it to parliament, barring exclusions made on security grounds).

The Security Service Tribunal investigates complaints about the Service made by the public. The tribunal is made up of 3 senior members of the legal profession, appointed by the Royal Warrant. The Tribunal and Commissioner are both independent of the Government. The service and staff are under a legal duty to hand over any records considered necessary to investigate the case; service personnel can also be interviewed. Grounds are established for unlawful records to be destroyed and the complainant compensated.

The Security Service Commissioner has the additional capacity to investigate cases where although the complaint isn't upheld, s/he believes the service has acted unreasonably.

The IOCA Tribunal and Commissioner act in a similar manner to other agencies like HM Customs and Excise. The Tribunal can additionally quash an ongoing warrant and destroy copies on intercepted communications.

RELATED AGENCIES

The Security Services works closely with a number of other government organizations

Secret Intelligence Service (SIS/MI6): The external intelligence service shares pertinent information with its internal sister agency

Government Communications Head-Quarters (GCHQ): Provides signals intelligence from around the globe that may be of vital interest to the internal security agency

Home Office: The Home Secretary regularly issues warrants and the service provides national threat warnings daily

Joint Intelligence Committee (JIC): Sets the national priorities in terms of intelligence

Ministry of Defense (MOD): The service vets new military recruits and defense contractors

Police Forces: The service is actively in contact with all of United Kingdom's 55 police forces, mainly through *Special Branch* and regularly liaisons the *National Criminal Intelligence Service* dealing with major crimes and organized crime activity

Royal Ulster Constabulary (RUC Special Branch): Providing Northern Ireland intelligence for arrest purposes

Other bodies of interest include *HM Customs & Excise*, the Northern Ireland Office, Foreign and Commonwealth Office, other armed service units and over 100 foreign intelligence services

The role of the service can be broken down into 4 areas…

Investigate – to obtain, collate, analyze and assess intelligence about threats
Counter – to act, enable others and counter specific threats
Advise – to keep Government (and others) informed, advise appropriate responses and suggest internal security measures
Assist – to provide assistance to other agencies, departments and organizations

Executive Powers: The civil servants of the service have no legal right to carry firearms, or to arrest suspects. This legal delineation under law seeks to diminish the powers invested in an MI5 officer, who may be tempted to transgress due process (as they have relative freedoms as intelligence operatives beyond the scope of police officers). The Security Service works closely with the Special Branch Units of all 55 UK based Police Services in arresting individuals.

Warrants: The Home Secretary will only issue warrants for wiretapping or interception of mail or clandestine searches if the service can prove that national security is endangered, the action will gain substantive information and the operation cannot be reasonably achieved any other way. A formal written submission is needed under the Interception of Communications Act 1985 (IOCA).

Intelligence as Evidence/Law of Disclosure: In line with the widening remit of helping out police services with terrorism and serious crimes, provisions have been made under law for the disclosure of evidence by Security Service personnel. The Criminal Procedure and Investigations Act of 1996 recognizes that the duty of disclosure must accommodate the need to protect sensitive information (that might damage national security). Yet, it also makes clear that intelligence investigations should have the same duty of care to stay within the law in terms of their investigations.

Files: The registry is kept under tight controls, only certain review bodies have access to content in the review of complaints about the security services operations. There are currently 440,000 files in the registry established since 1909. 75,000 have never been investigated (only opened due to protective security advice), which leaves around 290,000. 270,000 have been closed (of which 40,000 have been converted to microfilm). This leaves 20,000 active files of which (13,000 are UK citizens + 7,000 are foreign nationals such as spies or terrorist members). Files are kept for a non-specified length of time (as the Security Service Tribunal might require records for various complaints). However, the process of removing old files from WWI has taken place, the Public Record Office has taken possession of a large batch of these. This process has been accelerated after the end of the Cold War.

Threats: The major threat pertinent to the UK at the moment is the activities of Islamic extremist organizations, such as Al-Qa'ida. Under the sponsorship of Osama Bin Laden a number of terrorist activities have been perpetrated against Western targets. With a large population of Muslims within the London and Birmingham area, a great deal of time is currently being devoted to becoming aware of any possible provocative actions made by the service that might inspire a new breed of homegrown terrorists.

Northern Ireland despite being relatively quite after the signing of peace agreements in the late 90s, is still a major area of operational concern. Rogue elements in the Republican cause (the Provisional IRA, Continuity IRA and Irish National Liberation Army) continue to actively pursue aborting the fragile peace process, and the Security Service knows there may be yet more bloodshed to be played out on the streets of Northern Ireland.

The Russian Mafia and many other organized crime organizations still look toward the United Kingdom as a place to smuggle weapons, drugs and people for profit. It is of special concern that many organized crime activities these days seem to be linked to terrorist causes. Irish sympathizers fore-instance, have sought to import drugs from South America to add cash to their cause.

Another major concern is the availability of enriched uranium and weapons of the former Soviet Union on world black-markets. It is considered a viable threat to the world's major population centers, that eventually a nuclear device may be triggered by a terrorist group in a place such as London.

Staff: There are currently estimated to be around 2,400 full time staff employed by the Security Service of roughly equal proportions of males to females, around 50% of which are under the age of 30. Around 150 individuals at any one time are seconded or attached to other similar departments and agencies. The breadth of staff roles include management, clerical staff, lawyers, linguists, computer experts, communication specialists, scientists, technical staff, building maintenance staff, catering staff, printers, drivers, mechanics and porters. Of course, there are the usual *tradecraft* experts. A number of specialists are recruited straight from industry or specialist research activities.

Recruitment of Staff: The service seeks to mainly recruit specialists, graduates and school leavers into its programs. All candidates are vetted by the service (Developed Vetting DV process) to the highest level of clearance. Since 1997 the service has actively advertised for new recruits and specialists, candidates applying for the Civil Service Fast Stream programs can nominate the service as their preferred department.

Training: The service seeks to maintain training opportunities for all staff. There is a structured induction training process and mentoring programs. There are additional programs available to develop specific skills for specific posts. The Graduate Scheme for intelligence officer's lasts over an intensive six-month period (including spells of training and work experience) – this period is provisional employment. The opportunity exists to study for relevant external qualifications, as well.

Staff Forum: A Staff Forum of elected representatives from across the service, serves as a channel of communication for staff issues such as pay and employment conditions. They regularly hold formal meetings and representatives are available to discuss employment issues privately.

The Staff Counselor: All members of the Security Service (and SIS & CGHQ) have access to an external Staff Counselor. Due to the nature of their work, such a service guarantees confidentiality from their employer, and maintains the secrecy of their work. A report is sent annually to the Prime Minister and relevant Secretaries of State detailing any particular areas of concern and the levels of stress members of staff have been exposed to.

Equal Opportunities: The service has in place policies and staff to maintain recruitment and promotions adhere to selections based on merit.

Anonymity of Staff: Other than the public announcement of the Director General (since 1992), the Service seeks to maintain the secrecy of all staff. Due to the nature of their work, staff could face personal threat if their names were to be put into the public domain. Even long after an intelligence officer has left the field of operations, exposure might endanger the lives of informants, other officers and threaten ongoing investigations. In criminal trials Security Service staff give evidence anonymously, behind protective screens. Indeed, there is even reluctance from staff to be subjected to this degree of exposure, unless their appearance as a witness is absolutely necessary (under cross-examination they may inadvertently give up operation techniques or other vital information).

Note: This practice is similar to precautions taken by undercover detectives or specialist police officers.

Budget: The services budget paid from the Single Intelligence Vote (SIV) each year, this provision is set aside for the purposes of the three UK intelligence agencies (MI5, MI6 & GCHQ), the proportion given to each agency is determined by Ministers (usually in relation to Joint Intelligence Committee (JIC) recommendations). However, in recent years close scrutiny is paid to making the service run cost-effectively.

Permanent Secretaries' Committee on the Intelligence Services (PSIS): Ultimately, the arbiter of the SIV package every year is a Committee chaired by the Cabinet Secretary, containing members of the Permanent Secretaries (including the Home Office, Foreign and Commonwealth Office, Ministry of Defense and Treasury). They scrutinize the annual budgets of all three services, expenditure forecasts, plans and intelligence requirements.

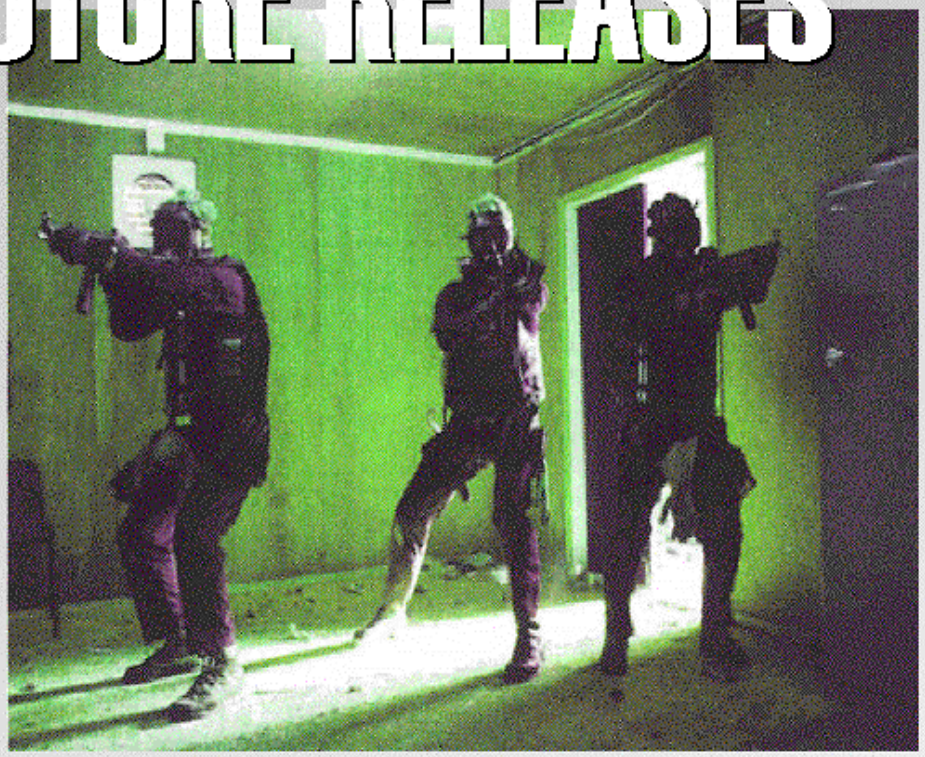
National Audit Office (NAO): This government department audits expenditure to ensure that the Service keeps in line with forecasts, the accounts are certified by the Controller and Auditor General.

Oxbridge Gentlemen's Club: In recent years the service has sort to remove the image of Intelligence Officers being recruited solely from the two most prestigious Universities in the United Kingdom (Oxford & Cambridge). In 1997 the Service sought to advertise for new recruits through major UK newspapers. Over the past 20 years efforts have been made to change the image, age and ethnicity of the service – especially necessary with the changing nature of the threats to Western countries. The hard drinking image of old is also a bit of a misnomer, despite such activities being synonymous with such high pressure jobs, efforts have been made to institute new levels of fitness amongst officers and ancillary staff.

Paperwork: Another aspect regularly mentioned about working at the Security Service is the overzealous nature of the paperwork. Although efforts have been made to speed up some aspects of service procedure by computerization, a lot of work is still necessarily committed to paper – it is often crucial in such roles to keep paperwork up-to-date and accessible

Games Master Challenges for running MI5 Agents: The nature of the service restricts the rights to arrest and to carry firearms, it may hamper opportunities for *closure* in operations. This may be obviated somewhat by having the players make a second Special Branch officer to close in and make the arrests. A further possibility is to allow for a catastrophic event similar to 9/11 to take place, and have emergency powers enacted by Parliament to give Executive Powers to MI5 operatives, working in the area of Counter-Terrorism.

FUTURE RELEASES



Spyglass Productions hopes to add further modules for your gaming enjoyment in the future, here is a rundown of the planned accessories

OCTOBER/NOVEMBER 2005

A ROUGH GUIDE TO PARAMILITARY ORGANISATIONS

Enter the world of terrorism, freedom fighters and separatists
Discover the motivations and tactics of the 21st Centuries most notorious extremists...

MID YEAR 2006

A ROUGH GUIDE TO UNITED STATES MILITARY/INTELLIGENCE SERVICES

Enter the world of the FBI, CIA and the famed Navy Seals...

LATE 2006

A ROUGH GUIDE TO BRITISH MILITARY/INTELLIGENCE SERVICES

Enter the world of MI6, MI5, GCHQ and the legendary SAS...