EXTRACTS FROM EYE SPY INTELLIGENCE MAGAZINE

** images are presented in low-res screen shots for quicker loading*

E S P I O N A G E

Special Tradecraft: Much of the information contained in the following features relates to spycraft, recruitment and the real world of intelligence. There is also a fascinating look at infiltration, Field Stations, 'spy recruiters' and what might happen if you become a 'person of interest'.

TITLE: DARK ARTS 2 - INFILTRATION & UNDERCOVER

SUB TITLE: METHODS TO INFILTRATE, COMMUNICATE, OBSERVE AND CONCEAL

ISSUE 44

Creating layers of "reality", "assurance" and "insurance" are areas deemed off limits to those not working in the intelligence business, but there are a few trade secrets in the public domain already, and these do provide a glimpse of how a sting operation is enabled... Eye Spy examines the complex and dangerous world of undercover agents, the forwarding of intelligence, and some of the methods used to communicate, infiltrate, observe and conceal...

EXTRACT ONE:

Depending on the environment, everyday circumstances and, often the country of operation, working undercover and communicating intelligence can pose a major problem. Infiltrating a suspected terrorist cell, crime gang or any illegal operation with an embedded operative is both difficult and dangerous, but not impossible. In recent times at least six suspected terrorist cells in Canada, Britain and America, have been successfully infiltrated by actual operatives. In each case cell members had associations with al-Qaida.

To breach any terror cell's security the authorities must first try and establish who its core members are, the lead players and their association with each other. Beyond this, the group may use peripheral personnel who have some knowledge of the group's intent, though not necessarily be aware of operational plans, or indeed, the identity of all the core members. Many terrorist groups in the 1970s and 80s were small in number and confined to a specific area of operation. The Bologna (Italy) based group - Red Brigades - formed by student protesters who dedicated themselves to an "armed struggle" against the "capitalist state" were notorious for attacking government targets in the country. However, once an operative was caught, this often led to the capture of other terrorists. Today's terrorists are more cautious...

EXTRACT TWO:

Once a terrorist cell has been identified, its intent or role must be evaluated. Electronic and foot/mobile surveillance can expose a plethora of useful intelligence. Analysts will use this data to:

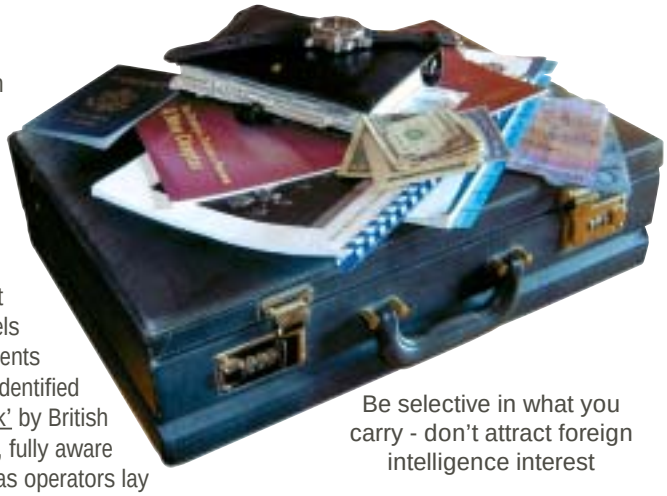
1. Identify core members.
2. Determine its role.
3. Assess the urgency of the investigation.
4. Learn of peripheral or support personnel.
5. Accumulate code words.
6. Identify meeting points.
7. Gather telephone numbers.
8. Check criminal backgrounds.
9. Discover if the group has an international thread.
10. Track and note electronic financial transactions.
11. Locate and disseminate Internet communications.
12. Determine members' specialist areas.

Acquiring a bar code number on a suspicious package could provide vital intelligence. Remembering such details when operating undercover is vital

TITLE: COUNTER-MEASURES - ESPIONAGE PROTECTION AND GUIDANCE FOR PROFESSIONALS ABROAD

SUB TITLE: SPY WARNING - DON'T SUCCUMB TO THE TRICKS OF FOREIGN SPIES
ISSUE 34

When a foreign intelligence service decides to focus its attention on businessmen, civil servants, diplomats and military personnel, it usually spells trouble. These stealthy spies could seek to 'turn' people using splendid **hospitality** or even provocative **'honey traps'.**



Be selective in what you carry - don't attract foreign intelligence interest

Attempts to befriend people staying in hotels may appear innocent enough, but certain hotels and apartments have been identified as 'high risk' by British intelligence, fully aware that overseas operators lay in wait for the unsuspecting guest.

When booking in to a foreign hotel, try and avoid adjoining balconies

Defence and industry contractors must also be wary of 'lavish hospitality', flattery and 'red carpet treatment', a common technique used by foreign intelligence networks to lure recruits. Once contact has been made and friendships sown, the person may continue to receive 'friendly emails' or correspondence, even on his or her return home. Intelligence officials note that suspect activity, which may start to become even more noticeable upon returning home, should still be directed to a worker's **security co-ordinator.**

MI5 say frequent travellers abroad should seek guidance on security matters and take particular care when transporting sensitive data. Before any outbound journey or business trip, persons should ensure documents and material contain no classified markings which could alert foreign intelligence agencies to the importance of their work. Laptop computers, diaries and notebooks are all prime targets...

TITLE: FIELD STATIONS AND SPIES

SUB TITLE:
ISSUE 40

Espionage and intelligence gathering are vital tools that dictate many decisions made by governments and military planners across the world. It is an ill-conceived notion that all spies work in an industry often depicted by Hollywood. In reality, the work of an intelligence-gatherer is time consuming and mundane. Nevertheless, in most cases it is interesting, vital, clandestine and for some, it can be dangerous or even fatal. A great deal of important intelligence is secured by officers operating in 'Field Stations'.

Both Britain and the United States operate **Field Stations** under the watchful eye of MI6 (Secret Intelligence Service - SIS) and the Central Intelligence Agency (CIA) respectively.

Staff liaise and interact with other security bodies, including diplomatic and military officials. Other countries have similar concerns, the former KGB called its overseas stations *"rezidenturas".* The term 'field station' or 'station house' is somewhat confusing and has led to the misconception that the intelligence services have actual offices in situ - a "walk-in front door". Though people do use embassies to defect via this method.

It is understood British field stations are classed from the high-risk Category A, such as Algeria, to the lesser B, such as Washington and New York, C, the European countries, and D, often the Commonwealth, where there is little or no threat. MI6 has approximately 50 operational field stations - the CIA perhaps as many as 100.

A station basically comprises of a number of officers assembled together who work on gathering and disseminating intelligence. It is their responsibility to understand, authenticate and quantify the data. In the case of MI6, the intelligence, sometimes referred to as "the product", is known as ***CX.*** This hails from the early days of MI6, its head 'C' in popular fiction, was Mansfield Cumming. These reports were regarded as top secret and marked 'Cumming Exclusively', abbreviated to CX. Today, such reports are prepared and forwarded to senior officials in London (MI6 headquarters). The CIA produces its 'product' for analysis at Langley, Virginia (CIA headquarters).

A field station also acts as a conduit for secret intelligence requests. Most, though not all, are 'housed' in the relative safe environment of US or UK embassies (the CIA also has a number of domestic stations located throughout the United States).

Working within an embassy compound provides additional security and privacy, not least because the building and personnel are protected under diplomatic law. Foreign security services are not permitted to enter the area unless permission is granted. In some environments that are considered safe, the station can be *'fronted'* by a seemingly legitimate business.

Intelligence is forwarded to MI6 headquarters situated on the River Thames in London

The size (personnel) of an MI6 field station is flexible and dependent upon various factors, including in-house diplomatic numbers, opportunities to gather intelligence, and the importance of the region. However, most stations are manned by about three or four intelligence officers from the **intelligence branch (IB).** MI6 has several hundred IB officers of whom approximately half are deployed overseas and are based at field stations. In the case of Britain, most CX is gathered by these officers. Besides IB or field officers, the station is supported by one or two general service or **GS** officers. Some larger stations cover areas **(zones)** which comprise of several countries. In times of conflict or heightened tension, it is not unusual to see additional 'specialist' persons joining a field station undercover in the guise of a diplomat. However, they are still vulnerable. Host governments can demand that named 'staff' be ejected. Usually, those asked to leave are suspected of espionage and may be field officers.

There are two types of station - **DECLARED** and **UNDECLARED**...

Everything you wanted to know about Field Stations in this detailed feature.

TITLE: DARK ARTS 1 - TRICKS OF THE TRADE

SUB TITLE: ENTERING THE OFFICIAL WORLD OF SURVEILLANCE AND INTELLIGENCE GATHERING

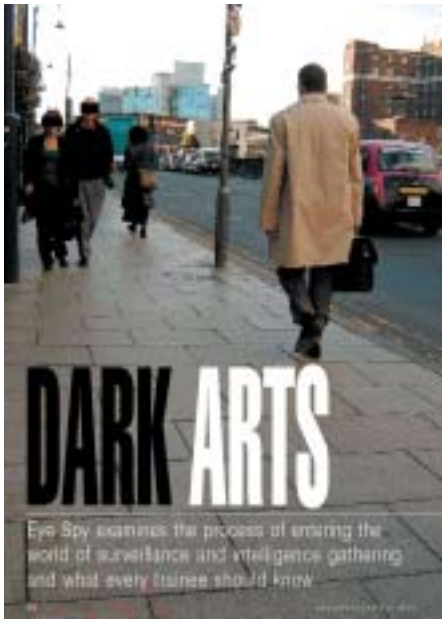
ISSUE 44

If you're interested in joining a government security service, then this feature is essential reading. From utilising your surroundings, training procedures, gathering intelligence, equipment use, family liaisons etc., countermeasures etc.

EXTRACT:

It's a question often raised by television news reporters following a terrorism scare - "how many surveillance officers are needed to monitor one suspect?" Intelligence analysts don't seem to able to agree on this one. Following recent operations in London, one expert said between 50-60 people, while another said 20 should be adequate. However, the truth is that the number is always dependent on the type of operation being performed, the seriousness of the situation, the location, and ultimately the organisational skill level of the target[s] being surveilled. However, it can also be governed by the number of officers available at the time. Without a proper analysis of all these factors (and there are many more), no expert can truly say how many officers are required.

In the last twelve months, MI5 has recruited over 250 people specifically for surveillance work. Training an MI5 surveillance officer takes between six-nine months, though again, this is dependent on various factors and the type of work that might ensue. Exercises to test the skill and determination of undercover intelligence operatives (both qualified and in training) regularly occur, and yes, they occasionally take place in cities and towns or the countryside to add an air of authenticity to proceedings. Other surveillance training takes place in specially constructed or controlled environments.

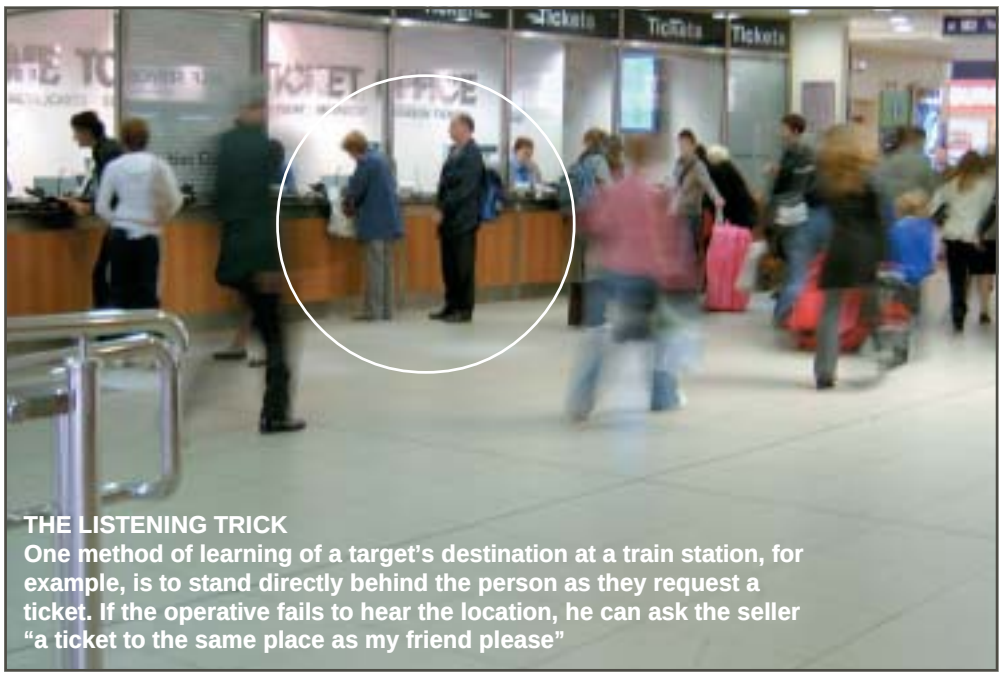


TRAINING

Before an ***'operative in training'*** is allowed to participate in real high-level operations, he or she must take various tests and learn the methods of their new employers. It's back to the classroom. Questions relating to fitness, eyesight and hearing are obvious. But what of the trainee's observational skills, or acting ability - essential in 'acting normally' in ordinary, unusual or difficult situations?

Training in the use of surveillance equipment is also necessary, so too is knowing how to wear or place covert devices. Many of these skills can be learned by training with a reputable agency, but when working for the government, there are 'new rules' and 'strict guidelines' to follow.

Then there is physical appearance. If a 7ft 9inch tall person seeks a career in street surveillance, he must either be brilliant or be able to walk quickly with a stoop, or mask his height in ways that are not obvious. And that's not easy. However, size, height, age, race, religion or colour are not negative factors and each in itself could prove invaluable in different operations.



THE LISTENING TRICK
One method of learning of a target's destination at a train station, for example, is to stand directly behind the person as they request a ticket. If the operative fails to hear the location, he can ask the seller "a ticket to the same place as my friend please"

The subject of surveillance is huge and operatives can find work in other 'arenas', perhaps analysis, communications, photography or installing equipment. It's not just about street surveillance.

Three years ago MI5 bizarrely insisted in including a height restriction for prospective officers embarking on a career in this field. However, the same sort of code could

RULES

These images show what not to wear during a surveillance or undercover operation.

Far left: White training shoes may be comfortable, but they are very visible. The bag is cumbersome, colourful, large and carries a distinct logo that might be seen and remembered by the target.

Left: The white shirt worn by this officer in a training exercise stands out - especially against a dark backdrop.

apply to trainees with white or blazing red hair, or as one expert noted, the agent "was extraordinarily beautiful." All of these factors are manageable, of course, with a little help from disguise experts and trainers.

RULES

Coloured hair, wearing bright clothes or brilliant designer shirts with recognisable logos, white shoes....

TITLE: THE SPYING GAME

SUB TITLE: PERSONS OF INTEREST

ISSUE 45

The first rule of espionage?... There are no rules. If you have what they want, they will use any means to get it...

Eye Spy examines the unseen dangers for business people travelling abroad and provides a plethora of trade tips essential for defeating espionage. Interested in real tradecraft? Then don't leave home without first reading this feature...

EXTRACT ONE:

If you are sent abroad as a company representative armed with sensitive contracts or other important material, it's not impossible you will become a **'person of interest'.** MI5 and other security services offer guidance and advice on what to carry in terms of documentation, telephone numbers, letterheads and electronic data, i.e. CD-Roms, laptops or similar. That's absolutely fine, but in most cases it's not practical to journey to a foreign land without your 'tools' - after all, if you're sent to Moscow to deliver a lecture or a presentation, these items are essential.

Venturing to foreign shores as a company representative, in most cases, means you will already be booked into a hotel. The reservation may or may not have been made directly by your employer. Most firms with ties to overseas countries use specialist booking firms, or increasingly, the Internet. However, in some countries, that information is forwarded immediately to the security services for analysis - henceforth, if you have been given the label of a 'person of interest', it's likely you will be monitored from the moment you arrive. That's not fantasy... it's a reality, especially in Russia, China, Iran and other nations. Hundreds of leading hotels

have an "arrangement" with the security services - usually via a senior manager or head of security. A few hotels are actually in the *'pocket'* of intelligence gatherers...

EXTRACT TWO:

THE PRIMED ROOM

A common trick often played out by hoteliers in the 'grasp' of many undesirable security services (or criminals) is the age-old - 'do not disturb' sign or 'room being attended'. Few guests re-enter rooms in the knowledge that everything is being 'set right', but such a situation affords those of ill intent with a genuine reason for being in your room for more than a few minutes. The *Hoover* will probably be turned on and the door locked - just in case you attempt to get in. If challenged, the maid will shrug her shoulders and make a quick exist... mumbling something as she departs... it's all part of the ruse.

Another trick for those wanting to search your personal belongings, or move you to another room (complete with an array of listening and monitoring devices - the **primed room**) is that of the faulty heater or air conditioning, jarred window, missing remote control for the television, dodgy plumbing etc. In genuine cases, the hotel will attend to these problems within minutes, but beware of the receptionist who states "it's too late - the engineer or technician is off duty - but we will sort the problem out as soon as we can." This means that if you have booked for more than one night you might be relocated to a 'primed room'. Don't accept the first room offered by the manager or receptionist.

EXTRACT THREE:

SOFTENING

Visiting a bar leaves a subject vulnerable to what's known in the trade as "softening". You're thousands of miles from home, it's a quiet night and a pretty girl or boy makes advances. Beware, it could leave you penniless, drunk, thus talkative, but more than that, a decidedly dodgy relationship might emerge that could lead to secrets being revealed, and worse... blackmail. The Russian and Chinese intelligence services are past masters at this type of activity. Similarly, beware of the hotel manager affording lavish hospitality, it could be genuine, or a ruse to gain your confidence and friendship. The same rules apply to taxi drivers. A number of hotel chains are in league with foreign intelligence services and are quick to designate or call taxis driven by agents. Few people ever question taxi drivers who ask personal questions. Indeed, be wary about giving exact details about your intended destination. CIA officers en-route to pre-designated meetings or locations will take time to digest a map and *walk that extra mile* - it's the advice given to many overseas travellers on 'intelligence business'....

TITLE: DARK ARTS 3 - THE RECRUITERS

SUB TITLE: THE STRANGE WORLD OF INTELLIGENCE RECRUITMENT

ISSUE 45

Since 2002, it has been estimated that Western security and intelligence services have recruited an additional 50,000 personnel to predominately counter al-Qaida's global terrorism. However, for those wishing to join organisations like MI6 or the NSA, the road is not easy or initially rewarding, but without doubt the work can be unusual and absorbing. It can also dangerous for field operatives. For career personnel, length of service is beneficial. But just how difficult it is finding employment in an industry that still insists on absolute secrecy and loyalty?

Recruitment officers are unique in themselves, in that they are respected for their ability to identify people with an inherent skill to see beyond the conventional, or provide an exceptional opinion on affairs or situations. If you think is a little fanciful, think again, agencies will often surveill and track the progress of people with *'talent'* or persons in a position to assist by providing intelligence. Many agencies also

have 'liaison officers' who will be advised if a student with "exceptional ability" is spotted, be they in a university, premier technology company, have access to street 'secrets' or the media. The recruiters have an 'eye' for talent and will quickly discard those who simply won't be enticed, fall short of an acceptable level, or may turn out to be security liability. Beyond that, if a person can be of assistance in intelligence gathering, passive surveillance may ensue, engagement may take place and eventually their cooperation will be obtained. As many intelligence commentators note, "it can be a dirty business." Long gone are the days when recruiters would join a foreign language class in Oxford University to seek out potential talent - *but they may get a call from a teacher.*

EXTRACT:

A written application to MI6 will take anywhere between six to twelve months to process, unless you hold the codes to Russia's nuclear arsenal or the whereabouts of a hidden Iranian heavy water plant. During this 'waiting period' applicants may be forgiven for thinking their e-mails or letters have been lost, but that's not usually the case. Every response, statement and previous job or post will be checked, *if* you are a person of interest. Other agencies will telephone and confirm an application has been received. Assessors and analysts will reject 95 out of every 100 who apply - and very quickly. The 95% will almost certainly not receive a response due to confidentiality. For the lucky few even more checks will ensue - some dating back to school years. If by chance a letter or phone call is received from agencies like MI6, then a location for an initial meeting will follow - this is generally regarded as the 'first interview'. Don't expect any response to include more than a few lines - and forget the letter-headed paper. It's possible you will be contacted in person, though this is highly irregular. MI6, however, are quick to point out on its website that applicants should not get too disheartened by rejection: *"The application process for SIS is extremely competitive and many candidates fail. Sometimes this is because candidates lack the relevant experience. We welcome reapplications from candidates who have gained additional qualifications or experience since their last application. Usually candidates should wait for at least two years before reapplying."*

An essential feature on what to expect when you apply to join the intelligence world...

TITLE: THE MEDIA AND SPOOKS

SUB TITLE: EMBEDDED SPIES, INTEL STORIES AND AN UNEASY RELATIONSHIP
ISSUE 42

The intelligence services, acting on government instructions, are increasingly conducting operations that some editors and media commentators deem wrong and probably illegal. Meanwhile, government ministers and even presidents have accused the mainstream media of threatening national security by publishing details of on-going intelligence operations. Eye Spy examines the reasons why both entities need each other and what could happen if relations break down altogether. Also an interesting look at media infiltration, how to ascertain what's authentic or just propaganda, and Britain's unique D-Notice.

EXTRACT:


THE MEDIA AND SPOOKS
EMBEDDED SPIES, INTEL STORIES AND AN UNEASY RELATIONSHIP

In times of conflict, the media often acts like a conduit for national propaganda. The BBC can be cited as a classic example during WWII often *bending* the truth to keep the public spirits high. True, major newspapers and television stations are controlled or owned by persons who have their own political agendas and bias, but when the nation is threatened, even those who oppose government policies, prime ministers and presidents, set aside their differences and work to a common theme - at least most of them.

Providing information to the media via press statements and scheduled conferences is a useful exercise in investigation, diplomacy and good manners. In the United States, agencies like the CIA, FBI and NSA have websites that portray a willingness to be more open. The UK's MI5, MI6 and GCHQ have all followed suit, and other countries security services, often mistrusted by the media and public have realised that 'information flow' should be a two-way affair. Just how much information to impart to the public and media is still a subject of debate. But the newspaper and television industry is a cut-throat business and one scoop can generate extra finance and great acclaim. So what happens therefore, when an 'intelligence whistleblower' approaches a journalist with a story that is controversial and previously unknown? It often depends on how friendly the managing editor is with, for example, 10 Downing Street's press secretary, or the White House spokesman. Naturally, legal advice is sought, but in some cases calculators appear - how much additional revenue will be raised by "a story" against the fines that might be incurred or an injunction for publishing tales of murky dealings, exposing undercover lives, or relevant to this magazine - on-going or projected intelligence operations?

DEDICATED LIAISON

Major newspapers across the globe have individuals with direct telephone numbers to the intelligence world. In some cases, a **'dedicated liaison'** is in place who can request or provide the security services with information....

TITLE: SHREDDING YOUR IDENTITY [IDENTITY PROTECTION]

SUB TITLE: THE SCOURGE OF THE SPY COMES OF AGE
ISSUE 33

For criminals, acquiring new identities and lining one's pocket at the same time from credit card fraud has become relatively easy. Creating a cloned credit card from details secured from a stolen card takes minutes. Machines and the software necessary to perform this task are available from dubious sellers all over the world. The machines are easy to set up and can read the magnetic strip of any card and with a little know how - can bypass most security systems. It's not a subject the banks like to discuss, though they are coming under increasing pressure to produce the 'totally secure credit card'. These controversial machines simply take the data and import it on a new card. An expert can produce a new card ready for use in about 10 minutes. Unfortunately the card will work on 99% of all ATMs in any country. Such machines are not strictly illegal to own or sell, but using them for such activities will result in a prison sentence. Terrorists and criminals are simply undeterred by the threat of prison, for the rewards are great.

Your credit card data appears on most receipts, gas, shopping etc. Even if some digits are not printed, criminal software can soon insert the missing numbers. Restaurants are perhaps the biggest culprits. Your details are usually printed in full, and on more than one occasion, workers have been known to sell your card information. It seems incredible that many shoppers casually discard receipts on the floor, or at the foot of ATM machines. For those who drop them in their home garbage beware - there are persons working in the underworld who are actually employed to sift through rubbish **(trash trawlers)** and locate your card number and bank statements.

Eye Spy provides a plethora of sensible tips, including Internet guidance, office and home security to stop criminals acquiring your belongings and even your identity.