

LEAD BY THE WORLDWIDE INTELLIGENCE COMMUNITY

THE COVERT WORLD OF ESPIONAGE

EYE SPY



WANT TO BE A SPY?

- INFILTRATION • GOING GREY
- SURVEILLANCE • BUGGING • ACTING

GAS LIMOS PROJECT

DEADLY PLOT TO KILL THOUSANDS IN THE UK AND USA

NEW SERIES

DIY EYE SPY

BUILD YOUR OWN SPY TOOLS

- CYBER TERRORISM
- LETTER BOMB ADVICE
- U-BOAT ENIGMAS RECOVERED
- MI6's MYSTERIOUS CREST
- INTELLIGENCE DIGEST



WIN A COVERT
CAMERA
DETECTOR

VOLUME VI NO. 44 2006 USA \$5.99 CANADA C\$7.99

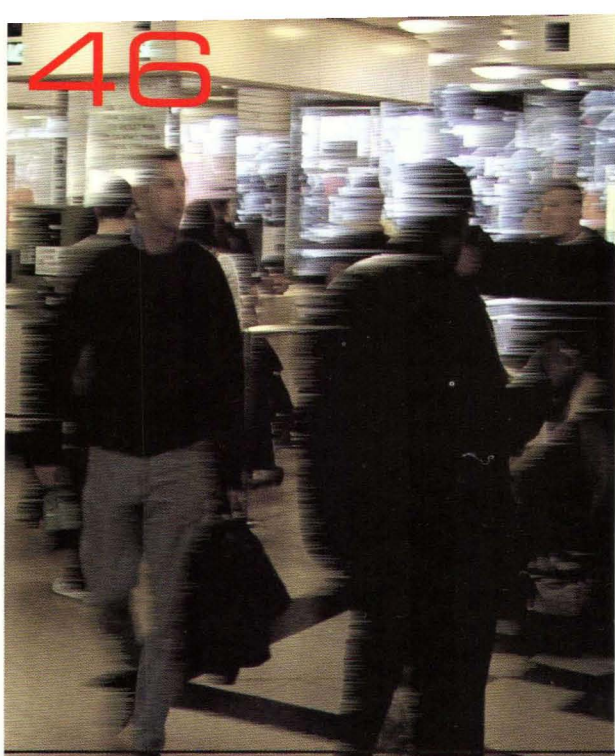


THE REAL MI5 SPOOKS



Printed and Published in the UK

46

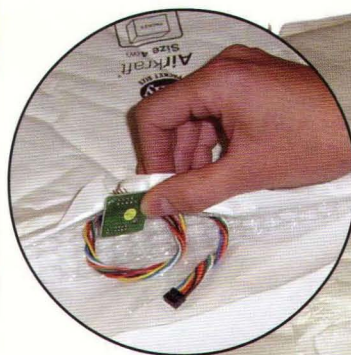


INFILTRATION

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...

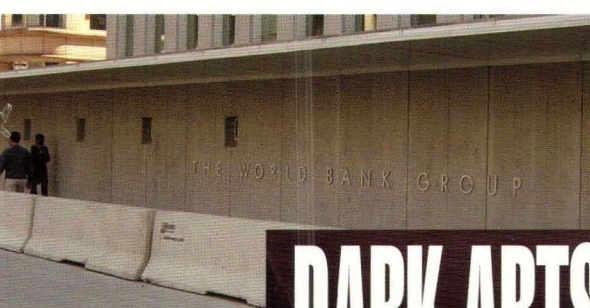
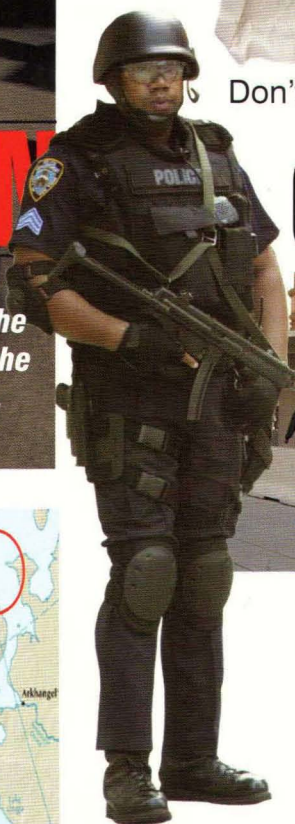
MAIL SURPRISE

42



Don't be surprised by your mail this Christmas

GAS LIMOS PROJECT



In 2004, al-Qaida's brilliant codemaker was arrested... information found on a computer led police to London and the 'GAS LIMOS PROJECT'. MI5 discovered plans to bomb several buildings in the UK and United States, including the World Bank headquarters in Washington DC...

26

DARK ARTS

32

Eye Spy examines the process of entering the world of surveillance and intelligence gathering and what every trainee should know

PAY AS YOU GO ESPIONAGE

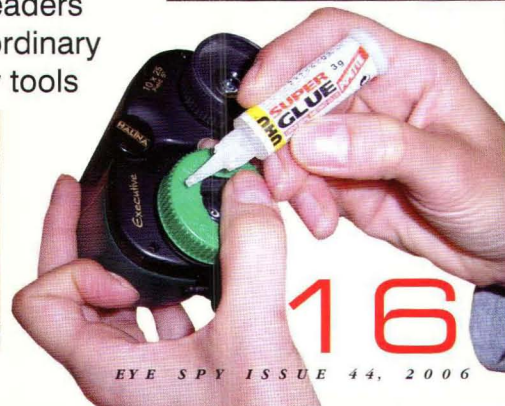
54



The contract 'spooks' plying their trade across the globe

EYE SPY DIY

New Series where readers can build or convert ordinary instruments into spy tools



16

EYE SPY ISSUE 44, 2006

EYE SPY

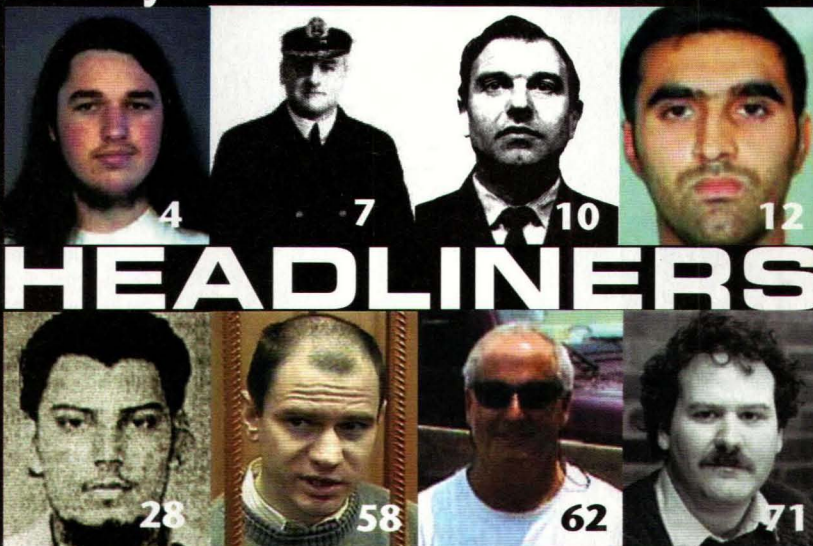
C O N T E N T S

- 6** Mystery of MI6's Crest - Solved
The mysterious 'brain' crest attributed to Britain's Secret Intelligence Service is authentic
- 10** A Spy's Blood Money
A European Court rewards George Blake - one of Britain's most notorious spies for his treachery
- 12** The Parliament Plot
Details unravel of an al-Qaida operation that mirrors a 400-year-old plot to blow up the Houses of Parliament
- 18** Barnham - Photo Special
In the late 1950s, Britain redesigned an air base to store its nuclear missiles. Its life was short lived, but visitors to a sleepy area of England can still experience its eerie past. The story of Barnham
- 52** Bridge to North Africa
MI5 and Scotland Yard raid a London restaurant and arrest several suspects of trying to recruit civilians to al-Qaida terror cells in North Africa
- 56** Winter Cometh
A few tips from our surveillance experts that will keep your windscreen clean, your body warm, and details of an interesting product just in case nature calls
- 58** MI5 and University Spying
A leaked report suggests MI5 is finalising plans to help universities spot suspected terrorist recruiters using the campuses of seats of learning to recruit students
- 62** The Enigmas
A fascinating story about the recovery and restoration of WWII Enigmas from the German U-85 sunk over half a century ago. David Hamer reports from Fort Meade
- 68** Cyber Terrorism
Kevin Coleman examines the evolving threat of cyber terrorism - its history, destructive power and the steps that can be taken to halt the hackers. Part 9 of the series - 'Understanding Intelligence'
- 78** PowerMonkey - Product Review
An absolutely terrific device that is set to take the market by storm - the PowerMonkey - an emergency battery charger that can be used anywhere

EYE SPY is published eight times a year by Eye Spy Publishing Ltd.
All rights reserved. No part of EYE SPY may be reproduced by any means wholly or in part, without the prior permission of the publisher. Not to be resold, lent, hired out or disposed of by trade at more than the recommended retail price.
Registered Company No. 4145 963 Registered for VAT. ISSN 1473-4362



Test your observation skills



HEADLINERS

- 4 Azzam the American • 7 Sir Mansfield Cumming • 10 George Blake
- 12 Omar Khyam • 28 Noor Khan • 58 Igor Sutyagin • 62 Roger Hunting
- 71 Fred Cohen

some inside features

4 Intelligence Briefings; 8 Intelligence Extra; 24 Intel Trade Book Store; 30 Back Issues;
58 Intelligence Extra; 60 Subscribe; 74 Book Releases; 80 Eye Spy Trade Shop

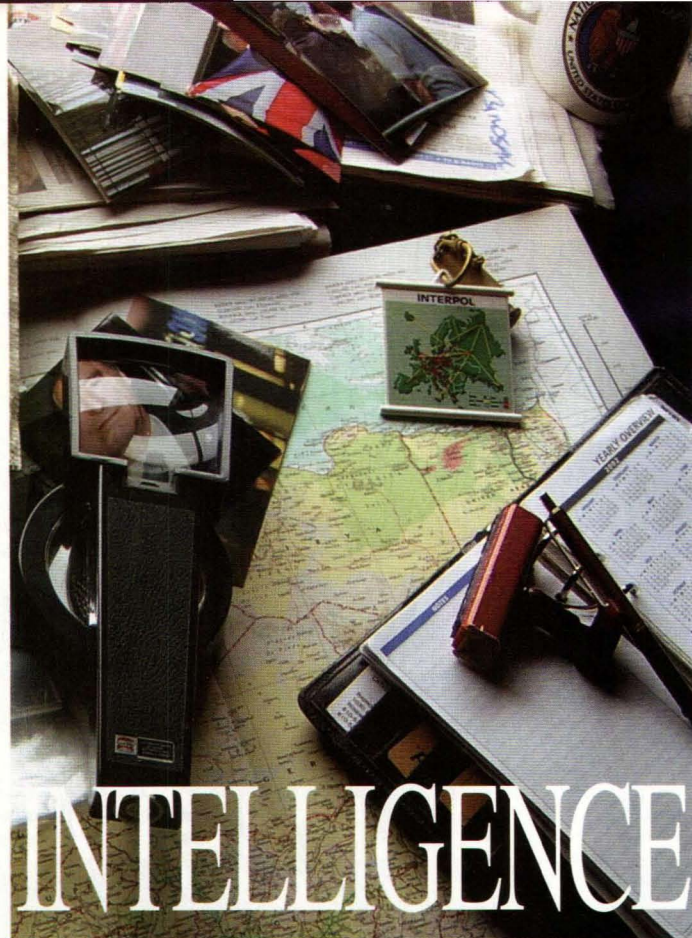
EYE SPY EDITORIAL

In this information-packed edition of Eye Spy, readers will find three specially commissioned features on tradecraft and the intelligence services. We receive dozens of enquiries each month from readers wanting to learn more about the training potential operatives undertake as they endeavour to carve out a career in the security services. So what's it really like? Training techniques are carefully guarded secrets, but we can relate basic scenarios and reveal a few tips from the real spooks who ply their trade in countries across the world.

A new series of DIY Spycraft begins in this edition. In coming issues readers can learn from our experts who have spent years adapting ordinary devices and turning them into more powerful tools. Use the material responsibly!

There's just time for me to mention our new subscription card. All new and existing subscribers can use the card to save money on selected items. Wherever you see the card, the item is discounted for subscribers. See page 23 for more information.





INTELLIGENCE

THE AL-JAZEER

Two former UK officials face April trial for Al-Ja

A date has been set for the trial of former Cabinet Office spokesman David Keogh and former parliamentary researcher Leo O'Connor, who are accused of violating Section 3 of Britain's Official Secrets Act by leaking a secret memo in which President Bush was said to have told Prime Minister Tony Blair in April 2004 of a plan to bomb Arab broadcaster Al-Jazeera at the height of the US campaign against Iraqi insurgents in Fallujah.

Journalists will be banned from the trial, according to a ruling made by Judge Richard Aikens back in July 2006.



© LAW ENFC

American Charged With Treason

Azzam the American becomes the first US citizen charged with treason since WWII

Adam Gadahn, a 28-year-old California man has been charged with treason and providing material support to a terrorist group for making a series of propaganda videotapes for al-Qaida, including one in which he praised the hijackers involved in the 9/11 attacks and referred to the United States as "enemy soil." Gadahn is the first person to be charged with treason against the USA since the World War II era.

The charges filed in the Central District Court of California say Adam Gadahn, also known as 'Azzam the American', "gave al-Qaida aid and comfort... with intent to betray the United States."

In October the FBI added Gadahn to its Most Wanted Terrorists List. The US Department of State is offering a reward of up to \$1 million for information leading to Gadahn's arrest.



Aliases: Abu Suhayb Al-Amriki, Abu Suhail Al-Amriki, Abu Suhayb, Yihya Majadin Adams, Adam Pearlman, Yahya, Azzam the American, Azzam Al-Amriki



"Adam Gadahn represents a new breed of home-grown extremist, who has chosen to betray the country of his birth," FBI Executive Assistant Director Willie Hulon said during a press conference in Washington DC.

Gadahn appeared in a videotape broadcast in 2004 in which he identifies himself as "Azzam the American."

A former resident of Orange County, Gadahn appeared in a series of videotaped segments that were broadcast between October 2004 and September 2006. In the first tape, Gadahn is wearing black sunglasses and a headdress wrapped around his face. He identified himself as Azzam the American and announced his relationship with al-Qaida. "The streets of America shall run red with

AFFAIR

'Bombing' memo leak



Keogh and O'Connor are alleged to have disclosed part of a transcript in which Prime Minister Tony Blair apparently resisted a proposal by President George Bush to bomb the Qatar-based satellite station - this after the station broadcast images of civilians lying dead in Iraq.

According to the charges, Keogh allegedly gave the memo to O'Connor at some point between 15 April 2004 and 29 May 2004. The *Daily Mirror* then ran a story relating to the affair, noting that 'sources' "disagreed as to the seriousness" of Mr Bush's suggestion.

A White House spokesman called the report "outlandish and inconceivable." Downing Street said it had "no information" about any proposed US action against Al-Jazeera.

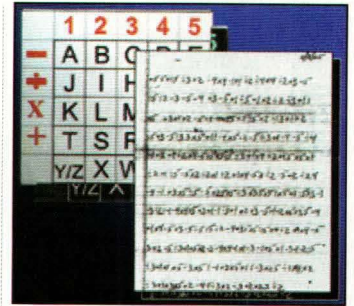
Both Keogh and O'Connor deny the charges.

CASE OF THE CODED CLUES

Breaking jail man's code reveals deadly clue

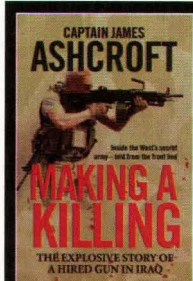
In jail awaiting trial for the abduction and murder of 11-year-old Carlie Brucia in 2004, Joseph P. Smith wrote an enciphered message to his brother. In it, Smith replaced letters of the alphabet with a series of one or two-character combinations of numbers and symbols. He also wrote the message from right to left, starting at the bottom of the page and working his way up.

The letter was sent to the FBI Laboratory, where cryptanalysts quickly deciphered the code, which held incriminating references to hiding evidence and moving the girl's body. It also contained an admonition to keep quiet: "DESTROY THIS AFTER DECIPHERING IT AND SHUT UP." Smith was



convicted in 2005 and received the death penalty for his crimes.

The case was one of the many investigations last year by the Laboratory's Cryptanalysis and Racketeering Records Unit. And it's one of scores of investigations and success stories contained in the Laboratory's 2005 Report.



MAKING A KILLING

THE EXPLOSIVE STORY OF A HIRED GUN IN IRAQ

AVAILABLE FROM EYE SPY

Ref: ES/1174

UK £20.00 USA \$40.00 ROW £22.00



blood," Gadahn said on the 2004 broadcast.

In a broadcast in 2005, around the fourth anniversary of the 9/11 attacks, Gadahn called the attacks "blessed raids" and discussed the "jihad against America." Earlier this summer, Gadahn appeared in a videotape that also contained statements from al-Qaida leaders Osama bin-Laden and his deputy, Ayman al-Zawahiri. More recent propaganda broadcasts aired on 2 September 2006 and on the fifth anniversary of 9/11.

FBI Deputy Director John Pistole said Gadahn's indictment for treason and material support for terrorism prompted his elevation to the Most Wanted Terrorists List. "Gadahn is considered a high value target, which puts him high on the FBI's radar screen," Hulon said. "This intense exposure limits Gadahn's operational ability, but he still poses a different kind of threat as a communicator for al-Qaida."



FBI Deputy Director John Pistole

Gadahn is probably in hiding in Pakistan or Afghanistan.

Gadahn's treason charge is controversial in nature and strikes a chord with the strange affair of fascist William Joyce, alias 'Lord Haw-Haw'. Throughout much of WWII, Joyce broadcast to Britain and America from his 'beloved' Germany - often mocking the public and government. Far from unnerving the populace, his bizarre rantings made him somewhat of a cult figure and his speeches were listened to by millions of people.

Joyce fled Britain in 1939 just one week before the outbreak of WWII - this after he was tipped-off he might be interned. He had already become a dedicated supporter of Adolf Hitler.

Friends in Germany put Joyce in contact with Dr. Erich Hetzler - Private Secretary to Germany's Foreign Minister von Ribbentrop. Two weeks after the outbreak of war he was appointed editor and speaker for the German transmitters for Europe at Berlin's Charlottenburg.

His infamous broadcasts began - "Germany Calling... Germany Calling" and soon the propaganda flowed. Tales of "betrayed Britons" and ghostly "fifth columnists" ensued. Throughout this period, his anti-semitism never stopped.

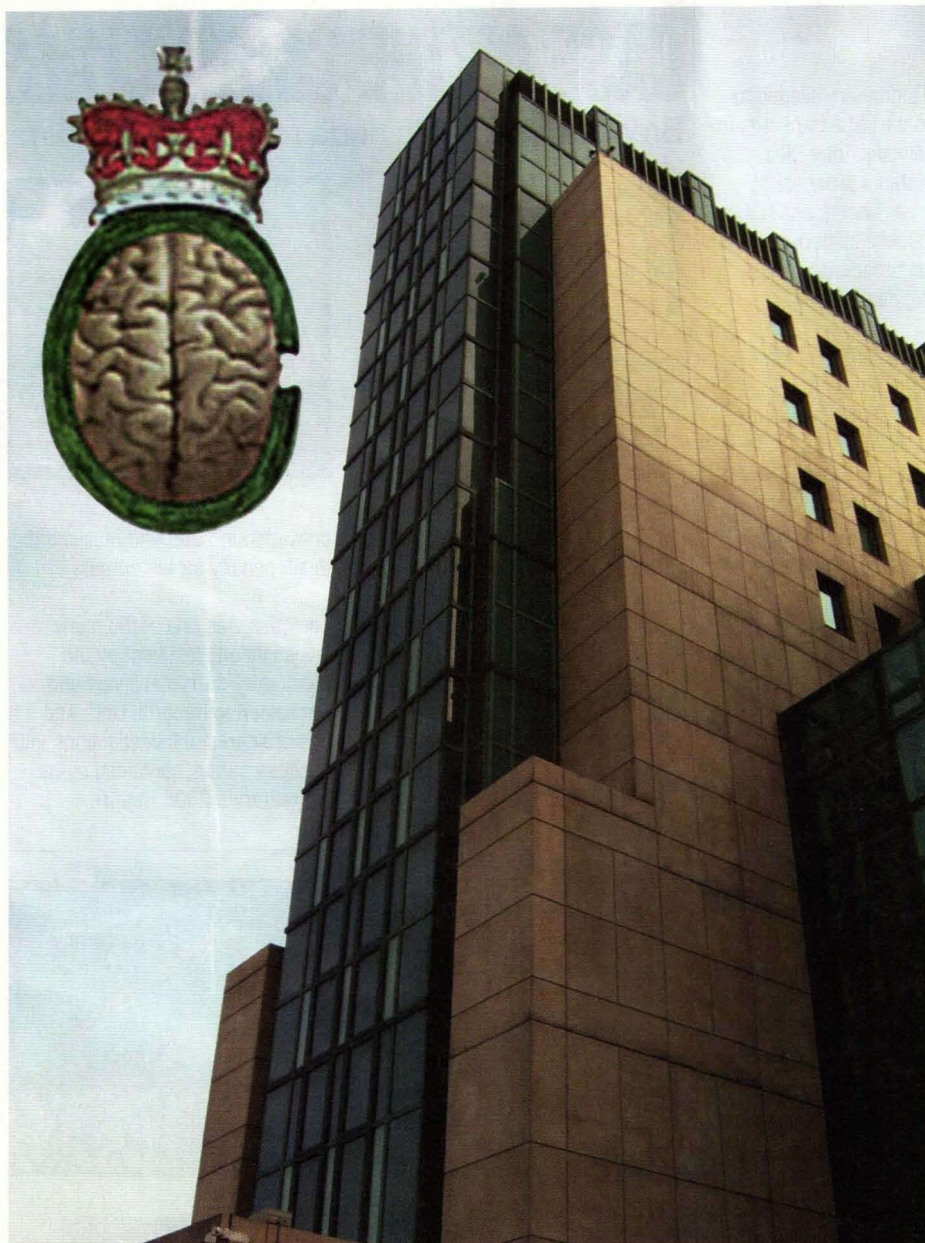
He was captured near Flensburg after the war and news of his arrest stirred-up hysteria in the press. The media immediately branded him a traitor. Interestingly, just one day before he was flown back to Britain,



William Joyce alias Lord Haw Haw

the Government passed the Treason Act 1945.

Charging Joyce with treason meant only one thing - death. However, it was not straightforward - Joyce was born in America, raised in Ireland and took German nationality on 26 September 1939. He was ultimately charged with treason from 3 September 1939 to 2 July 1940... the date when his UK passport expired. After his execution, Joyce was buried in an unmarked grave in the grounds of London's Wandsworth Prison.



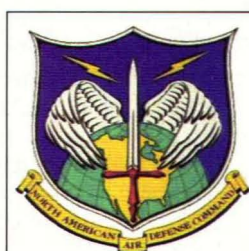
Sir Mansfield Cumming

(that's how it was identified) showing a grey brain encased inside a letter 'C' after its creator Mansfield Cumming, is authentic and still used by Britain's Secret Intelligence Service. It has never been officially acknowledged before, and still isn't. The only visual image on MI6's web site shows an SIS logo and UK Government crest - henceforth our description in Eye Spy 43. Prior to the feature's appearance, Eye Spy consultants agreed the crest was authentic, but obtaining any sort of official document displaying the crest was impossible. However, several immaculate sources have now confirmed it is real.



MI6 AND ITS MYSTERIO

Eye Spy's feature on intelligence and security crests certainly attracted a great deal of interest. So too did our giant intel crests poster which was warmly received by hundreds of readers. But not everyone was happy! Two Canadian intelligence officers wrote to say the NORAD crest should be flagged a joint USA-Canadian crest (on the poster it states USA). We also received a few e-mails from intelligence services wanting to know why their crest or seal never appeared. Unfortunately we did write to over 100 services but many failed to respond, or simply said "no crest exists". However, since then, many services have forwarded images so a new feature and second poster is being planned for next year.



The NORAD crest should also have been attributed to Canada

Spy will feature special forces and elite units in a future edition.

Yet we can now reveal what we have known for some time - the MI6 visualisation crest

We also received dozens of messages and letters from military personnel requesting a similar exercise be done for international armed forces. That's a huge task in that thousands exist! It's likely that Eye

The unusual crest mysteriously surfaced on the Internet about 10 years ago, and we are advised that even MI6 was puzzled who obtained and uploaded the crest. We can also reveal that other elements are missing.

The crest's origin dates back to the time of Captain Sir Mansfield Cumming RN, the Service's creator and first Chief. He used green ink to sign his letters, a tradition that continues to this very day. The colour green and the letter 'C' feature prominently in the crest of MI6. However, green has been a colour associated with intelligence since the First World War, thus it's impossible at present to say if the colour was incorporated to reflect Cumming's ink or the world of intelligence, though the former is likely! The letter 'C'



Semper Occultus

The crest which first surfaced on the Internet



It's likely the crest is inset. Evidence of air-brushing is apparent around the 'C', crown and text - *Semper Occultus*

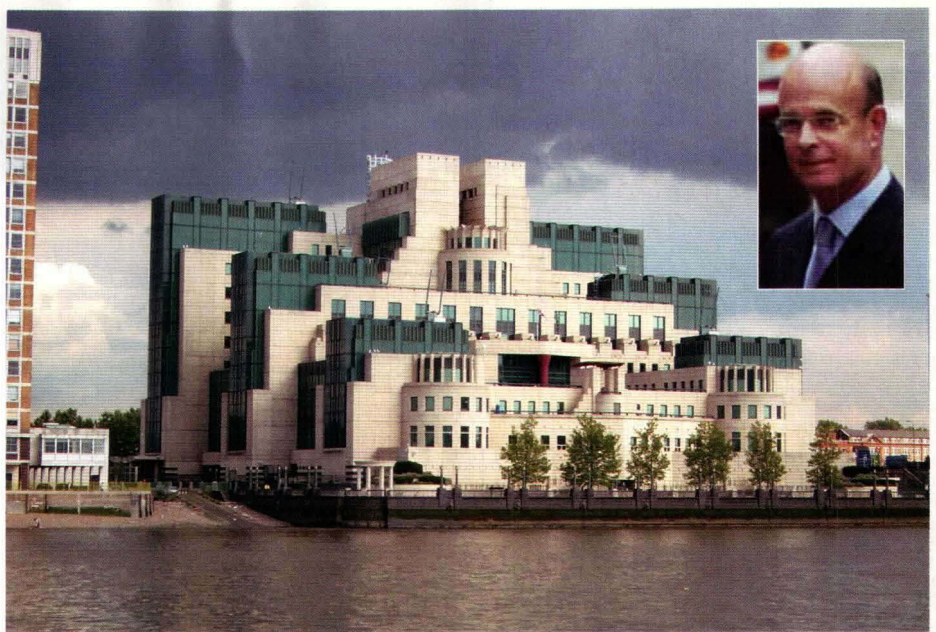
encases a drawing of a grey brain - almost certainly a direct reference to 'intelligence'. The brain symbol represents intellectual power and intelligence and the capacity to acquire and apply knowledge. Beneath the crest, two words are evident 'Semper Occultus' - translating to Always Secret - the ethos of the Service.

S CREST

Like 99% of all British Government services (both military and intelligence), the crest is topped by a crown. This refers to the Service's status as 'crown servants'.

It's quite possible that the MI6 crest is inset into the official UK coat of arms (used by the Service on its web site - see our diagrams). There is also evidence of 'brush work' on the crest that indicates it was surrounded by other details. This brush work is evident on the image.

Eye Spy is absolutely confident that the crest is authentic and thus ends one of the most debated and controversial topics amongst intelligence watchers....



THE SECRET INTELLIGENCE SERVICE

The Secret Intelligence Service (SIS), also known as MI6, collects Britain's foreign intelligence. The Service is based at Vauxhall Cross in London. Its current Chief is John Scarlett (above - inset). SIS provides Her Majesty's Government with a global covert capability to promote and defend the national security and economic well-being of the United Kingdom.

A BRIEF HISTORY

Britain's Secret Intelligence Service (SIS), more commonly known as MI6 (originally Military Intelligence Section 6), or the Secret Service or simply Six, is the United Kingdom's foreign intelligence agency.

The origins of the Secret Intelligence Service (SIS) are to be found in the Foreign Section of the Secret Service Bureau, established by the Committee of Imperial Defence in October 1909. The Secret Service Bureau was soon abbreviated to 'Secret Service', 'SS Bureau' or even 'SS'. The first head of the Foreign Section, Captain Sir Mansfield Cumming RN, signed himself 'MC' or 'C' in green ink. Cumming died in 1923, but his legacy lives on - all subsequent heads of the Service are referred to internally as 'C'.

Cumming sought to ensure that the Foreign Section of the Secret Service Bureau maintained a degree of autonomy but the War Office, in particular, managed to

exercise extensive control over his actions. The outbreak of the First World War in 1914 brought a need for even closer cooperation with military intelligence organisations within the War Office. The most significant manifestation of this was the virtual integration of the Foreign Section within the Military Intelligence Directorate. Thus, for much of the war, Cumming's organisation was known as MI1(c). This arrangement did not sit well with Cumming who regretted this diminution of his independence. As a naval officer he was less than pleased at appearing under the auspices of the War Office.

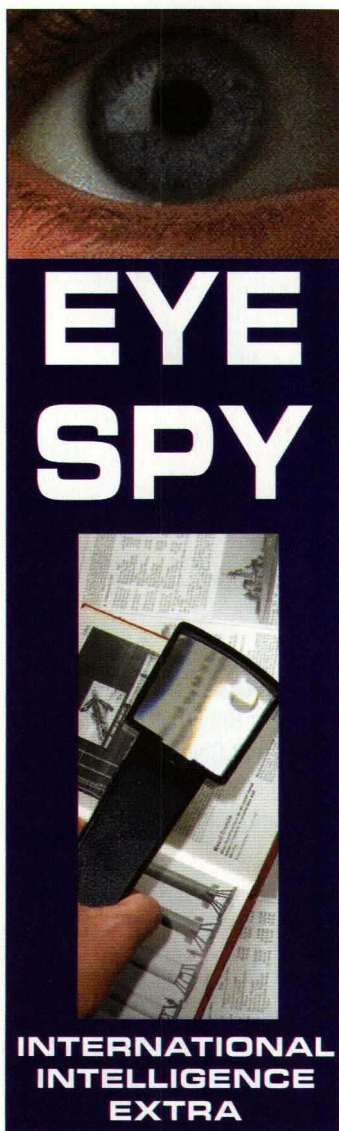
The debate over the future structure of British Intelligence continued at length after the end of hostilities but Cumming managed to engineer the return of the Service to Foreign Office control. At this time the organisation was known in Whitehall by a variety of titles including the 'Foreign Intelligence Service', the 'Secret Service', 'MI1(c)', the



The official UK Government crest

'Special Intelligence Service' and even 'C's organisation'. Around 1920, it began increasingly to be referred to as the Secret Intelligence Service (SIS), a title that it has continued to use to the present day and which was enshrined in statute in the Intelligence Services Act 1994.

MI6 has become an almost interchangeable title for SIS, at least in the minds of those outside the Service. The origins of the use of this other title are to be found in the late 1930s when it was adopted as a flag of convenience for SIS. It was used extensively during the Second World War, especially if an organisational link needed to be made with MI5 (the Security Service). Although MI6 fell into official disuse years ago, many writers and journalists continue to use it to describe SIS.



DELIVERY SYSTEM NEXT GOAL FOR NORTH KOREA

The US government confirmed that North Korea did carry out a nuclear test on 9 October. "Analysis of air samples collected on 11 October 2006, detected radioactive debris which confirms that North Korea conducted an underground nuclear explosion," said John Negroponte - the director of National Intelligence.

Just weeks earlier, Pyongyang successfully tested a number of long-range missiles, one of which carried coordinates for the island of Hawaii. Analysts warned that North Korea is within two-three years away from having a rocket capable of delivering a nuclear bomb. Analysts are also fearful the success of the test will prompt Iran to hasten its rush towards a nuclear device. North Korea, meanwhile, faces international sanctions.



Kim Jong-il



Border tension: A South Korean/US border control team monitor North Korean guards through binoculars

RUSSIAN-GEORGIAN SPY WARS

Russian 'spies' arrested by Georgian security services as tensions grow

In late September, five Russian military intelligence officers were arrested in Georgia for spying. The incident provoked a ferocious response from Moscow. President Putin demanded their immediate release. Shortly after the officers were detained, Georgian security services blockaded the regional headquarters of Russian forces in Tbilisi, the Georgian capital. The authorities also requested Russia hands over a "sixth spy". Russian Ambassador Vyacheslav Kovalenko said Moscow would not comply with the request. The men were reportedly involved in a spy ring of up to 12 Georgian citizens sympathetic to Russia - all the suspects were arrested. Officials described them as a "very dangerous spy chain." Russian ministers warned that "every action to free the suspected spies will be considered."

According to intelligence sources, the spy ring was headed by a Russian agent suspected of involvement with an explosion in the town of Gori in February 2005. Three police officers died in the attack.

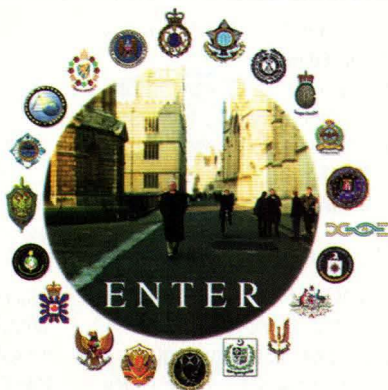


ESPIONAGE AND VODAFONE

ATHENS: Vodafone faces a huge fine over the Greek 2004 Olympic Games phone-tapping affair. Over 100 mobile phones, including those belonging to the Greek Prime Minister, Costas Karamanlis, leading cabinet members, high-ranking military officials and journalists were bugged by an unidentified agency by 'persons unknown' under the unprecedented surveillance scheme.

During the months leading up to the event, a huge security operation was set in motion. However, it seems not all countries were convinced Greece had every eventuality covered. An elaborate surveillance system was activated within software and used to intercept messages from Vodafone's Greek subsidiary. Officials say that "alarm bells rang" but no-one suspected anything. Eight charges of misconduct have been levelled. Vodafone could be fined a staggering £114 million (\$200m).

EYE SPY
INTELLIGENCE MAGAZINE
24 HOURS A DAY
www.eyespy.com



Welcome to **Eye Spy** Magazine

- SUBSCRIPTIONS
- EYE SPY INDEX
- SURVEILLANCE DEVICES
- PROFESSIONAL EQUIPMENT
- INTELLIGENCE BOOKS
- TRADE SECURITY BOOKS
- BACK ISSUES
- 24 HOUR NEWS SERVICE
- INTELLIGENCE RESOURCES
- SPECIAL OFFERS
- PHOTO GALLERY



21st Century Terrorism: A Clear and Present Danger

THE INTELLIGENCE SUMMITSM

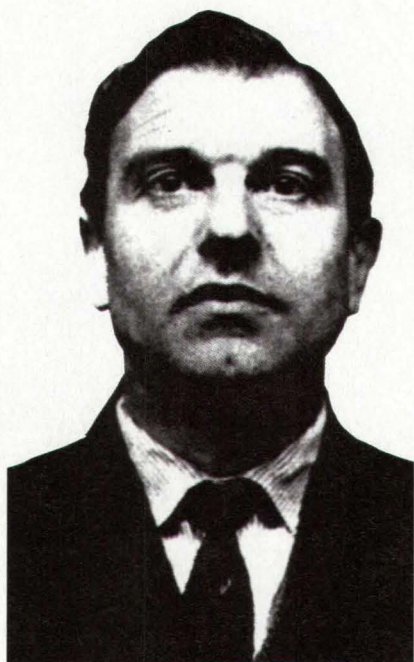
March 5 - 7, 2007

Hilton - St. Petersburg Bayfront
333 First Street South, St. Petersburg, Florida

www.intelligencesummit.org

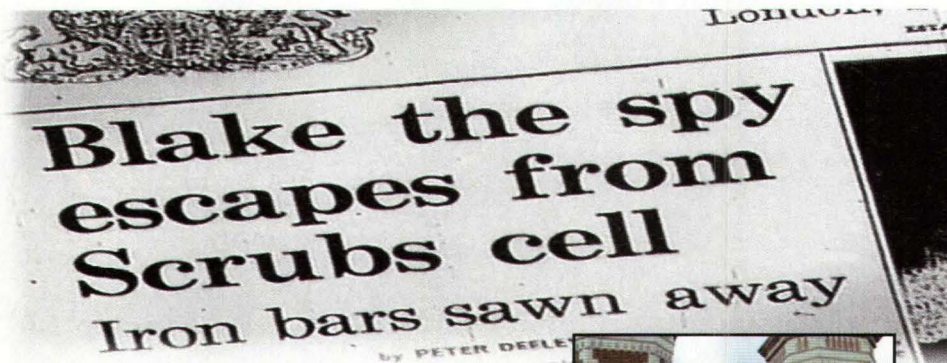
A SPY'S BLOOD

DOUBLE AGENT RESPONSIBLE FOR DOZENS OF DEATHS



One of the most infamous spies in British history has been awarded monies by the European Court for his treachery

George Blake, one of Britain's most notorious traitors responsible for the deaths of dozens of British agents has been awarded £3,000 (\$5,750) and £1,340 costs by judges sitting in the European Court of Human Rights. The court had heard: "The applicant had, they considered, brought the proceedings on himself as a self-confessed traitor who



wished to profit from his treachery." This still didn't stop the court ruling in his favour.

The money relates to profits over his 1989, autobiography, *No Other Choice*. A large section of the book focused on his work as an MI6 officer. Blake had already received about £60,000 in royalties before the UK Government started legal action to "stop him profiting from the book." A further £90,000 was frozen. In May 2003 his lawyers started another action and argued that his "human rights were being breached" - he was awarded £5,000 in compensation. Blake's lawyers had also argued that the case was being deliberately "slowed down" and passed through various courts. The Strasbourg court agreed. When news filtered through to 89-year-old Moscow-based Blake, of his recent award, he was "too ill" to understand the ruling.

Five years ago Blake failed in an attempt to obtain the outstanding royalties. An English court ruled that £90,000 should be donated to the charity - Save the Children. That ruling is not affected by the Strasbourg judgement.

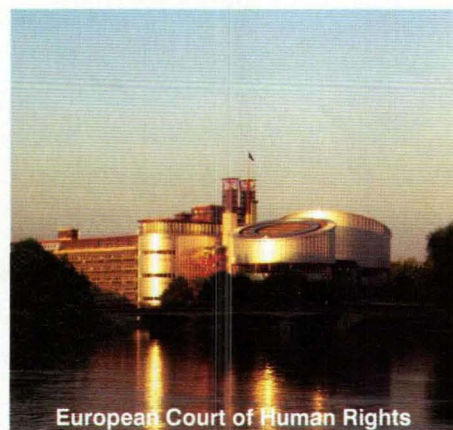
In 1960, Blake was "outed" as a KGB spy, but not before he had caused immense damage to British intelligence. Blake served in MI6 from 1944 to 1961, but unbeknown to his superiors, in 1951, started spying for the Soviets. At his trial (behind camera) in 1961, the UK Government initiated a clever plan to try and limit the damage he had caused from the media. They even suggested Blake, born in



Wormwood Scrubs Prison

Holland, had never been involved in intelligence work.

Blake was handed down a 42-year prison term, but only served five years after his dramatic escape from Wormwood Scrubs prison in London. Wardens found metal bars in a corridor had been sawn off and a rope enabling him to climb to freedom was still hanging in place. Despite a long search, he had disappeared - with the help of sympathis-



European Court of Human Rights

MONEY

REWARDED £3,000

Michal Goleniewski



Lt. Col Michal Goleniewski was the Deputy Chief of Polish Military Counter Intelligence until 1958. He also operated as a mole for the KGB in the Polish service.

By 1960 he headed Polish military intelligence in East Berlin.

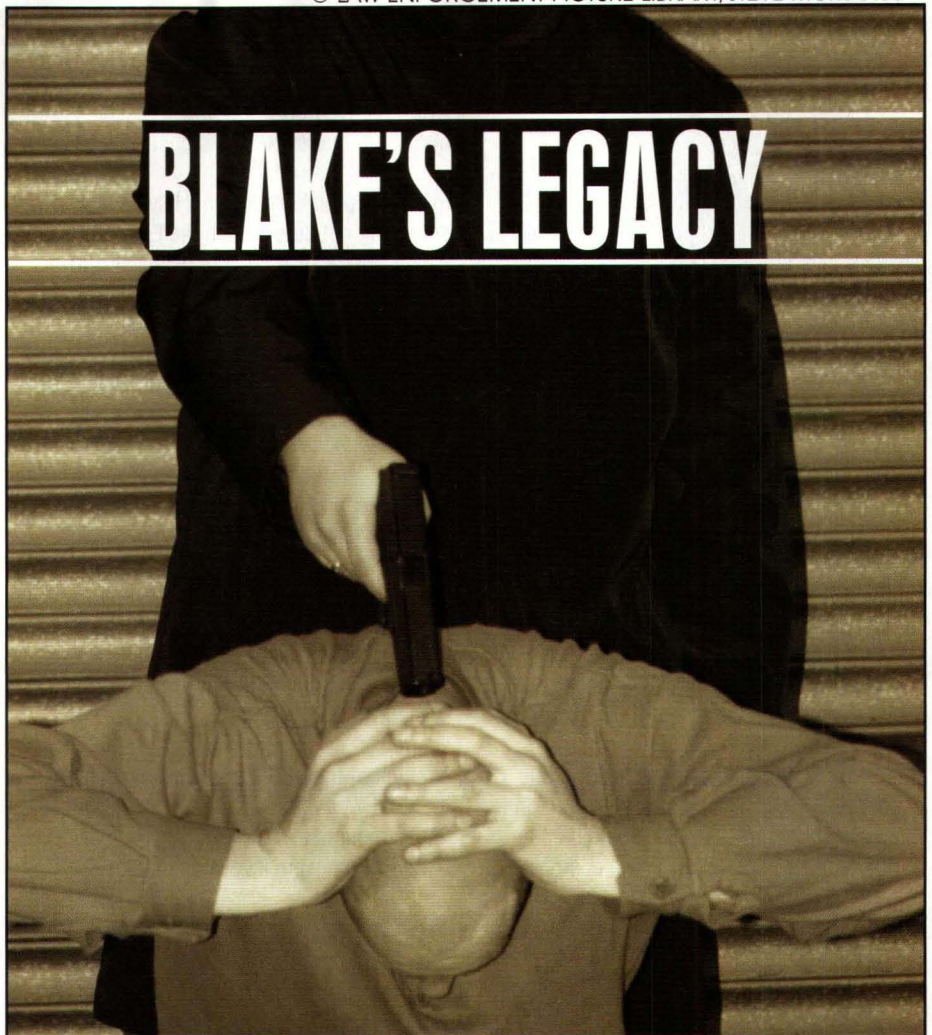
After his defection in 1961 Goleniewski told the CIA that George Blake was a double agent.

ers. A year later he surfaced in Moscow and was given a heroes welcome. Blake had left his three children behind and once in Moscow divorced his wife. He remarried shortly after and has remained in Russia ever since.

The spy's journey could not have been more colourful. The son of an Egyptian Jewish father, and a Dutch mother, Blake was interned



BLAKE'S LEGACY



GEORGE BLAKE (born George Behar) was born in 1922 in Rotterdam. After serving with the Dutch resistance he joined the British Royal Navy and in 1944 joined MI6. In 1949 he was posted to South Korea and upon the outbreak of the Korean War was interned by the invading North Korean forces. In 1951 he defected to the Russians, and volunteered to work as a Soviet Spy, being assigned the KGB codename Diomid. Information supplied by Blake to the Soviets enabled them to eliminate the entire Western intelligence force in East Germany between 1953 and 1955. It's believed he betrayed the names of more than 40 British agents to the Soviets. Many disappeared, and were thought to have been executed. Blake also informed the Russians about the American CIA intercept tunnel built from West to East Germany, and designed to intercept Soviet communications - a tunnel which the CIA believed to be a success until the truth was revealed following the dissolution of the Soviet Union some forty years later. Blake was identified following information provided by the Polish defector Michal Goleniewski in 1961.





Downing College, Cambridge

by the Germans before escaping and making his way to Britain. During WWII he joined the Royal Navy, before studying languages, including Russian at Downing College in Cambridge. His skills were noted by MI6 and he was sent to Seoul, Korea, as vice-consul under the guise of the Foreign Office.

He was arrested during the Korean war and spent three years in a North Korean prison. It was here his sympathies grew for Communism. A KGB official asked Blake to work for Moscow - but remain in MI6. Soon after, he returned to London and began handing his

KGB controller copies of every official document that came in his possession.

MI6 posted Blake to Berlin. He was tasked with searching out defectors in the East. He established a shop packed with "hard-to-get goods" on the border in the hope that Soviet officials would be tempted to enter. This afforded the KGB with an opportunity it could not have dreamed of. Blake said: "I was the only officer in Berlin who was actually in contact with the Russians." The KGB told Blake to send a communication to MI6 that he had befriended a possible defector who was willing to remain in place to provide intelligence. MI6 were delighted and forwarded questions to Blake to ask the "defector". From this ruse, the KGB learned of British policy towards the USSR and also had an opportunity to respond accordingly - disinformation flowed to the UK. The imaginary defector was an economist called 'Boris'. Learning the financial strength of the USSR was vital, especially as the Cold War was beginning to cost both sides huge amounts of money. Both NATO and the Warsaw Pact were involved in a race for

nuclear supremacy, it was advantageous therefore, to show the West that the USSR's economy was flourishing.

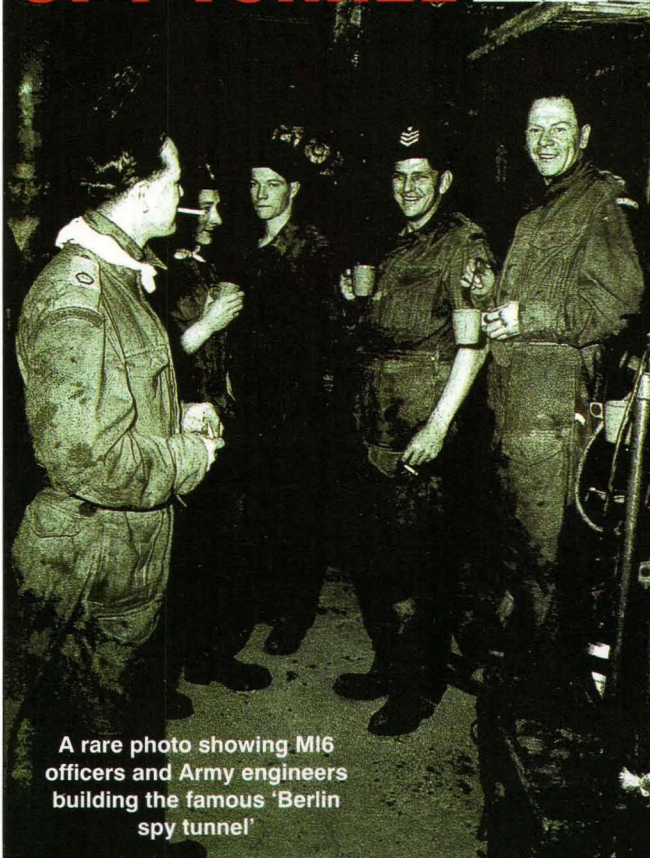
Renowned British (Australian born) intelligence expert Phillip Knightley, author of *The Second Oldest Profession: spies and spying in the 20th century*, is still uncertain if this was the case: "Was it to persuade the West to believe that the Communist economy was stronger than the West believed? Or weaker? To this day, no one in the West knows. And if Blake does, he is not telling."

- The UK's Department for Constitutional Affairs said it was obliged to comply with the Strausbourg ruling, noting that Blake had requested more money and that other claims were dismissed.



Blake pictured in Moscow in the late 1990s

THE BERLIN SPY TUNNEL



A rare photo showing MI6 officers and Army engineers building the famous 'Berlin spy tunnel'

The Berlin Spy Tunnel was one of the most astonishing and remarkable achievements of Western Intelligence during the Cold War. Built in the mid-1950s to tap into Red Army cables, it stretched some 800 metres underground from West Berlin to East Berlin. In operation for almost a year, it harvested an astonishing range of political, military and operational intelligence, including details of the political fallout behind the Iron Curtain from Khrushchev's famous denunciation of Stalin at the 20th Soviet Party Congress of February 1956, as well as information about Moscow's nuclear programme. Masses of data were gleaned about the Red Army's equipment, communications and morale, and what one CIA officer involved described as "a bonanza" of material about Soviet military intelligence and counterintelligence inside East Germany.

The tunnel was remarkable for another reason, too. Inside British intelligence, a Soviet 'mole' had betrayed it even before it was built. The plans were handed over to a

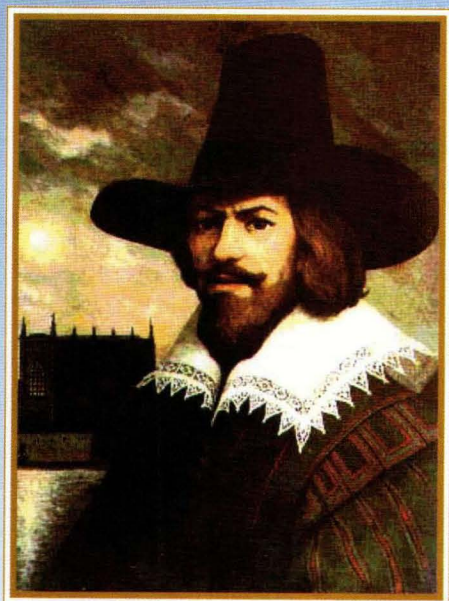
Soviet controller in London immediately following their approval by a top-level SIS-CIA meeting at 2 Carleton Gardens, the offices of SIS's Section Y which worked on intercepts, by the SIS officer George Blake.

For years after Blake's exposure it was assumed that his treachery had nullified the tunnel's achievements. Surely, the argument ran, the Soviets must have exploited the tunnel for deception or disinformation. Yet after the end of the Cold War, revelations from Moscow show that far from this being the case, the KGB preferred to guard the secret of the tunnel and protect their mole. As a result, genuine Red Army messages continued to pass along the cables.



OPERATION GREVIS

The 'Parliament Plot'



Exactly 401 years ago, Guy Fawkes, a Yorkshireman, conspired with a group of Roman Catholic conspirators to blow up the Houses of Parliament. He was caught and subsequently executed. His death is remembered every year by millions of Britons on 5 November - Bonfire night. It's ironic therefore that a trial is taking place just a few miles away from the UK seat of power that also involves another alleged plot to demolish London's most famous buildings. ➤



The London Eye

On the morning of 30 March 2004, anti-terrorist police arrested Omar Khyam and six other men after police discovered more than half a ton of ammonium nitrate fertilizer in a storage facility near Heathrow Airport in west London. The police operation was codenamed Crevice and owed its genesis to an alleged interception of an instruction sent by al-Qaida commanders to operatives in the UK.

The trial of Khyam is currently taking place at the Old Bailey and is not expected to end until



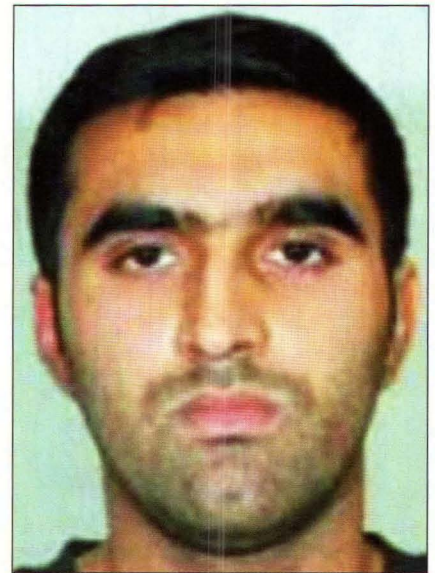
Security Service film footage of one of the suspects in the lock-up with the fertiliser

well into 2007. Some of the testimony is revealing.

On 15 September Khyam told the court: "I remember I was watching on a Wednesday, the Prime Minister's questions, and we just made a comment 'Can you imagine if you dropped a bomb right there and then? You would take out all the MPs'." Asked who had made the comment, Khyam answered: "I did." The other men just laughed. Defence barrister Joel Bennathan then asked: "Was that a serious proposition?" Khyam replied: "No."

Khyam said he felt happy when he heard of the 11 September 2001 attacks on the World Trade Center in New York, because "America was the biggest enemy of Islam."

The 24-year-old former university student denied claims by FBI informant Mohammed Junaid Babar that he discussed launching a bombing campaign in Britain. Khyam acknowledged that comments were made from time to time, but were only responses to what was

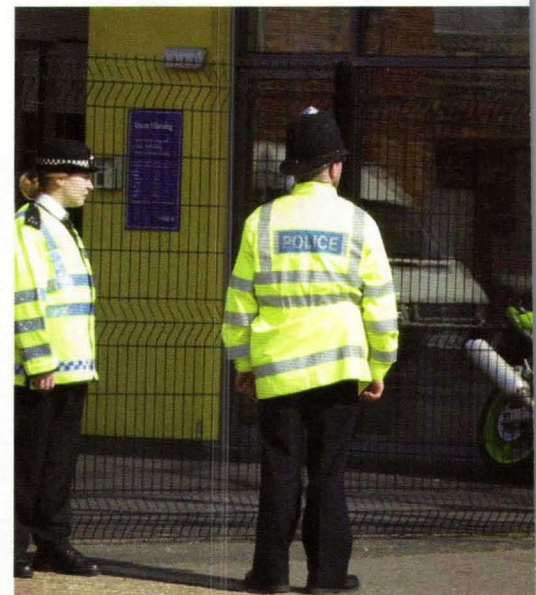


Omar Khyam

being said in the media. He said he was "working for the cause" in Afghanistan, bringing money and equipment from England.

He denied working for al-Qaida but accepted that people in the area could have had links to the terror group. Perhaps the most dramatic incident occurred on 18 September when Khyam was to be questioned about the purchase of the ammonium nitrate fertilizer. Asked by his counsel, Joel Bennathan, whether he had bought the fertiliser with the help of others, he told the court he could no longer answer questions because he was fearful of the well-being of his family in Pakistan.

Khyam said: "Before we go on to that topic, I just want to say the ISI in Pakistan has had words with my family relating to what I have been saying about them. I think they are worried I might reveal more about them, so right now, as much as I want to clarify matters, the priority for me has to be the safety of my family so I am going to stop. I am not going to



**Scotland Yard officers
raid the Access
storage centre near
Heathrow Airport**



© LAW ENFORCEMENT PICTURE LIBRARY/STEVE MCMANUS

discuss anything related to the ISI any more or the evidence."

Khyam said he attended a weapons-training camp in Pakistan where he claimed the country's Inter-Services Intelligence agency, (ISI), gave explosives instruction. He believes his family are in danger because of this admission. The ISI, according to Khyam, have already threatened his family - a claim dismissed by Pakistan officials. The jury has already heard that aluminium powder intended to be mixed with the fertiliser was found at Khyam's home in Crawley, West Sussex.

The court was adjourned for lawyers to consider the situation.

Another member of the alleged cell who actually bought the fertiliser admitted that he

knew it was for explosives. However, Anthony Garcia, 24, said he thought it was going to be shipped to Pakistan for use in Kashmir.

Garcia explained that in November 2003, Khyam asked him to buy the fertiliser. "He said he could not do it because he is Asian and might arouse some suspicion." He told the court: "At the time I thought it was really the same as fund-raising because I thought it was going to help people in Kashmir - to be used as an explosive, as a bomb. It would be basically to protect the villages under attack from the Indian soldiers."

Security officials believe the men had al-Qaida links and that they were planning a bombing campaign in Britain. Targets that have been mentioned include utility companies, The Ministry of Sound - a Soho nightclub, the huge

Bluewater shopping centre in Kent and the London Eye.

Khyam, his brother Shujah Mahmood, 19, Waheed Mahmood, 34, and Jawad Akbar, 23, all from Crawley, Sussex, Salahuddin Amin, 31, from Luton, Bedfordshire, Anthony Garcia, 24, of Ilford, east London, and Nabeel Hussain, 21, of Horley, Surrey, deny conspiring to cause explosions likely to endanger life between 1 January 2003 and 31 March 2004.

Khyam, Garcia and Hussain also deny a charge under the Terrorism Act of possessing 1,300lb (600kg) of ammonium nitrate fertiliser for terrorism. Khyam and Shujah Mahmood further deny possessing aluminium powder for terrorism.



© LAW ENFORCEMENT PICTURE LIBRARY/STEVE MCMANUS

EYE SPY DIY SPYCRAFT



Eye Spy launches its new series of professional DIY 'spycraft'

In the coming issues of Eye Spy we will not tell you where to acquire spy equipment - we will show you how to BUILD it - inexpensively and without needing a degree in electronics. These projects can be built with off-the-shelf parts and can be put together in a few hours - or in the following example - a few minutes. All the projects can be modified, mixed or matched to create an arsenal of spy tools.

Future projects include how to build a telephone voice changer, parabolic dish microphone, wall clock camera, bug detectors, room transmitter, night vision fire detector camera, outdoor night vision illuminator, spy camera killer and resurrect deleted data from a computer and many more devices associated with the world of espionage. Use the printed material responsibly.

DIY Long-Range Video or Camera



DEGREE OF DIFFICULTY



EASY



CONCENTRATE



TOUGH

Most micro or covert cameras offer very little in the way of telephoto lenses - they are designed to view a relatively close area with a wide angle lens. But, there are times when it may be necessary to monitor a distant scene, or it may be located in a hostile environment. Purchasing covert zoom cameras can be costly, and they often perform only moderately. Microcameras are designed to record as wide an angle without distortion. Even cameras that are available and equipped with zoom capability are often too underpowered to bring in a scene at more than a hundred feet.

Professional operators will of course circumnavigate the problem by purchasing expensive alternatives, but there is one method that costs absolutely nothing. Converting an ordinary £50.00 microcamera into one that can 'zoom-in' hundreds of yards is simple and takes between five and ten minutes.

The process involves mounting the camera to the eyepiece of a pair of binoculars or telescope. All that is required is super or hot glue, a few spare plastic lens covers or plastic caps. In our example, we used the tops from two milk containers.

Simply cut a hole in the lens covers or plastic cap of the binoculars and the camera; then

glue them together so that the camera can look into the eyepiece. It's that simple. The hole in the lens cap and eyepiece cover should be only large enough to allow the camera to see through the hole without any shadows in the video, and should be tested before gluing the caps or covers together. The covers should fit snugly over the devices so that there is no risk of dropping the camera if the binoculars are moved. If there is too much

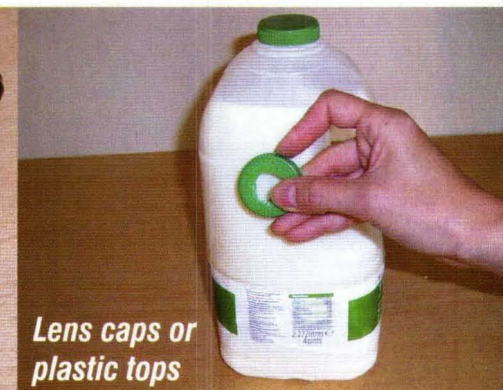
REQUIREMENTS



Binoculars



Camera - in this case wireless



Lens caps or plastic tops

play on either cap, an elastic band can be used to keep them in place. Covert cameras are very light and the likelihood of it pulling the glued cap away is slight.



The actual lens caps supplied with instruments such as binoculars are ideal, simply because they were built to protect the eye piece. But we found that a milk bottle cap fitted perfectly over our binoculars

When using your new 'long-range spycam', the easiest way to acquire video is to watch the live video on a monitor, as it will be brighter than what you can expect to see with the naked eye, especially if working with low-lux cameras. You may need to do some focusing by turning the threaded lens on the spy camera in whatever direction sharpens the image, usually counterclockwise. The picture quality is excellent and can be seen in the images which accompany this feature. Make sure you remember to focus the binoculars or telescope as well!

You can adapt these cameras to just about any device designed to magnify, including a telescope, gun sight or a microscope. There might be an occasion that you need to mark an object for identification so that it is undetectable to the human eye. By using a video camera attached to the microscope, you can make modifications by viewing the monitor and it allows you to make a record of the identifying marks or modifications

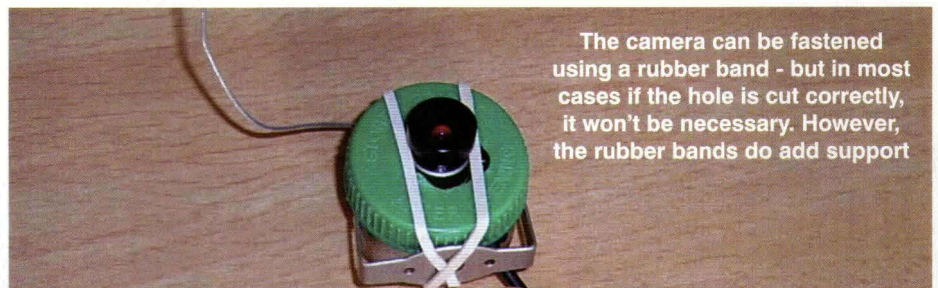
Continued on page 82

TEST IMAGE

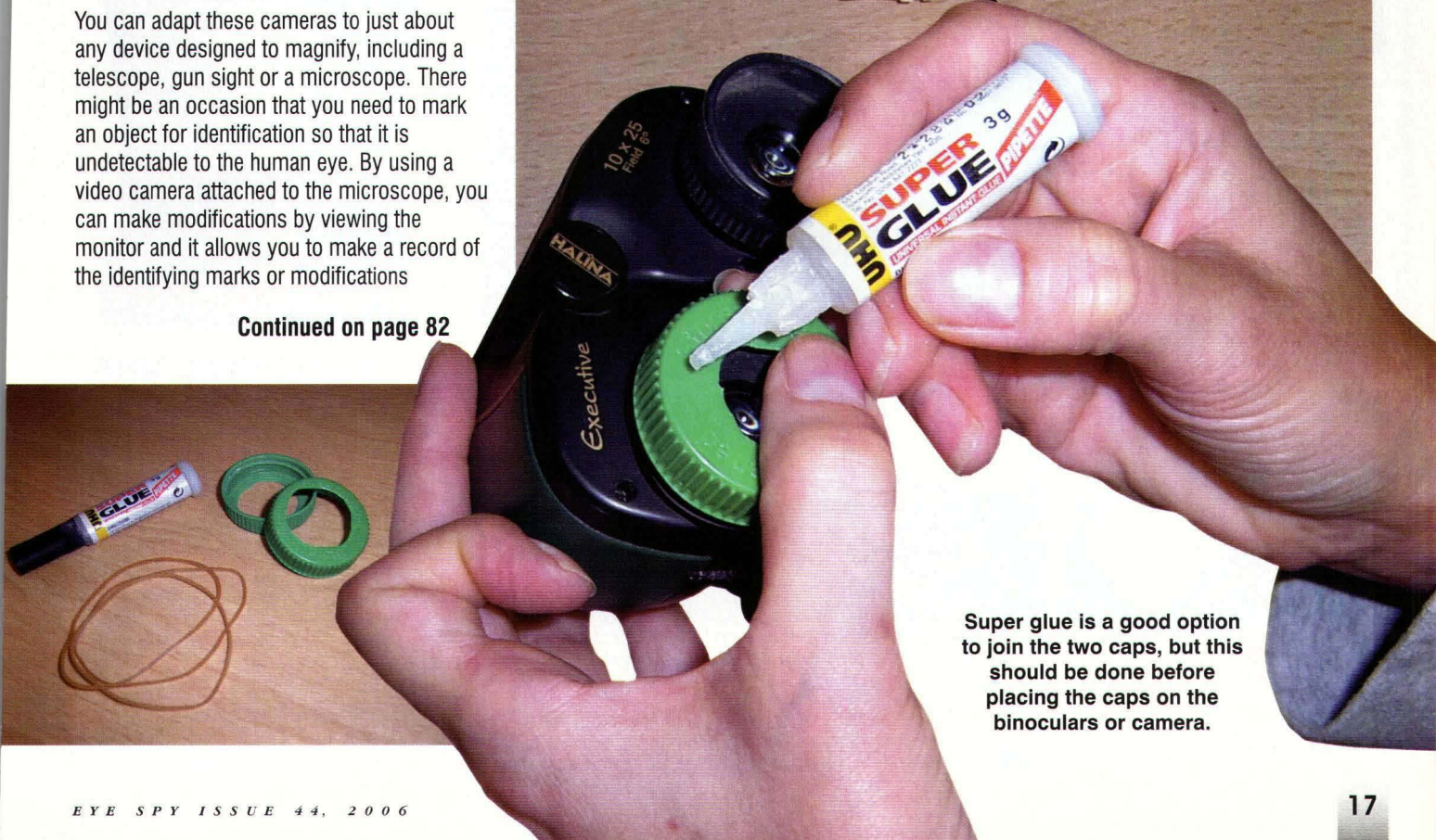


The camera never lies... or does it?

The target used in Eye Spy's test was a remote farmhouse tucked away in woodland. The untouched image shown here is a photograph taken off a monitor that was captured using the miniature camera seen on page 16. Blurry and hardly discernable - it was the best the camera could do. The distance from the camera is approximately 500 yards. Weather conditions were dry, warm with some sunshine and a little mist. The project took our researcher about five minutes to complete.... the results were dramatic. See page 82.



The camera can be fastened using a rubber band - but in most cases if the hole is cut correctly, it won't be necessary. However, the rubber bands do add support



Super glue is a good option to join the two caps, but this should be done before placing the caps on the binoculars or camera.

EYE SPY SHOP

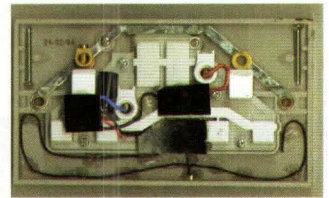
PROFESSIONAL

Professional surveillance and espionage equipment available from Eye Spy.
Check out our new range of products on: www.eyespy.com



**MAINS-DOUBLE
SOCKET
TRANSMITTER**

TRANSMITTERS & RECEIVERS



Using the identical UHF transmitter as the LH-1 (left), but inside is a fully working mains socket. This unit is ideal for permanent applications - easy to install. Continuous 24-hour-operation. Range 850ft.

Order code:
LS-TX-4 UK
£195.00

Only UK model available



UHF CALCULATOR TRANSMITTER

Working desk calculator conceals a tiny UHF transmitter. The unit can be left in an office environment without raising any suspicion. Range 850ft. Battery life of 15 hours. Use with any Eye Spy UHF receiver.



calculator model may be different to that displayed - but of equal quality!

Order code: LS-TX-6
UK £195.00 US \$350.00

UHF KEY RING TRANSMITTER

Ready to use in one second - Eye Spy's new key ring UHF transmitter requires the use of just one 3V lithium battery (included). Simply open the case, pop the battery in, and it starts transmitting immediately.



With a range of 650 metres, this remarkable bug can be left in offices, vehicles or just about anywhere! Use with any of our UHF receivers.
Sound pick-up - excellent.



Order Code:
LSSKR

UK £180.00
USA \$330.00
ROW £190.00

CREDIT CARD TRANSMITTER

This remarkable UHF transmitter is only 3mm thick and can be slipped in the side of a wallet, file, folder or pocket. It also has the advantage of voice activated transmission.

Battery operated (included)
Stunning quality. Range 850ft.
Use with any of our UHF receivers



**BESTSELLING
EYE SPY BUG**

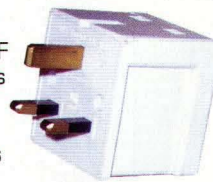
Order Code: LS-CCT UK £195.00
USA \$350.00 ROW £199.00

UK AND USA PORTABLE MAINS-DOUBLE PLUG ADAPTOR TRANSMITTER



United States model

A conventional fully mains-working double plug adaptor. Inside is a tiny UHF transmitter which becomes active and powered when plugged in. 24-hour-a-day transmission. No batteries needed just plug into any socket. Minimum range 850ft. Sound pick-up - superb. Use with any Eye Spy UHF receiver.

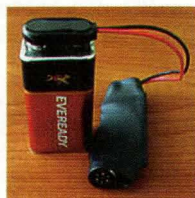


UK model

Order code: LH-1
UK £195 US \$350

please state which model you require

UHF BODY WORN TRANSMITTER

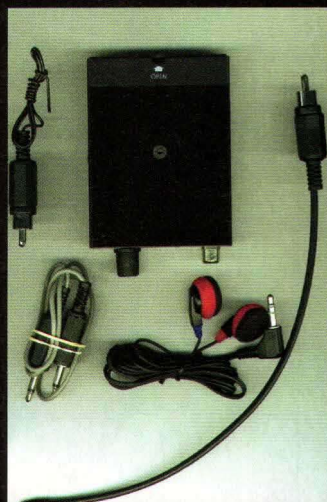


Built by
specialists
and used
across the
world

Bodyworn or for a room this UHF miniature transmitter is superb. The 6mm diameter microphone can even be pushed under door gaps to listen to sounds in another room. Use with our UHF receiver which will programme to receive transmission. Range 850ft.

Order code: L-IR1 UK £125.00 US \$230.00

10-CHANNEL METAL CASED UHF RECEIVER UNIT



Order code: L-SS-12CR
UK £145.00 US \$290.00
ROW £155.00

Eye Spy's superb 10-channel UHF receiver kit that can be used to pick up transmissions from any of the transmitters listed here. The unit will pick up transmissions from different UHF listening devices placed in several locations, simply by changing channels.

Powered by a 9v battery, the unit has a range of 400 metres - comes with jack-plug so you can record transmission and luxury earphones for privacy - all contained in a solid case.

FOR OUR FULL RANGE OF TRANSMITTERS
AND RECEIVERS VISIT www.eyespy.com



10-CHANNEL UHF RECEIVER AND TRANSMITTER KIT

This transmitter and receiver (metal cased) kit is ready to use in seconds. Our tiny matchbox-sized room transmitter, is extremely sensitive to sound and can be concealed absolutely anywhere. It will pick up voices up to 40 feet away and transmit with amazing clarity to the receiver. Powered by one 9v battery. Transmitter range 850ft.

Comes complete with all accessories.

UK £290.00 US \$575.00



WARNING: Some of the products advertised in this magazine may be illegal to operate in your country. Please familiarise yourself with the law as it affects you.



SECRET BRITAIN

Tucked away in the glorious English countryside is a former military facility that hides a plethora of Cold War secrets...

Watch towers, crumbling concrete huts, barbed-wire fences, seemingly oddly designed pathways and roads and a number of strange buildings indicate this was no ordinary facility. Eye Spy takes a look at what remains of **RAF BARNHAM** - a former top secret base once used to house Britain's first nuclear deterrent... the Blue Danube ►



BARNHAM

The Cold War base with a unique and shadowy history...

It's one of the most fascinating Cold War military locations in the UK, though visitors unaware of its existence would ever believe it once hosted Blue Danube, Britain's first nuclear bomb. Today, the primary buildings of what was RAF Barnham - a dispersed subsidiary of RAF Honnington in Suffolk, act as Gorse Industrial Estate. However, there are still many structures in place that reveal its secret history - a location once capable of storing well over a 100 fissile cores. Just inside what was the main electronically controlled gates, a high concrete blast wall still sits tall and a massive watch tower in immaculate condition gives some sense of scale to its role. It's one of the first features you notice that betrays its previous role, but all the buildings have a distinct "military feel" even though some now host small commercial businesses.

Situated around the main compound in woodland, some 60 concrete buildings, sometimes called kiosks, hutches or huts (about the size of a shed) on Thetford Heath stand empty in well-managed terrain. The kiosks design was such that it was intended to cast a tree-like shadow, presumably to foil Soviet detection from the air. It's a thoroughly eerie place to visit, especially when you consider each hut hosted a material so deadly in nature. Building of the so-called pentagon-shaped 'bomb store' (23 acres) began in 1953 and was finished by 1955. The main storage buildings were divided into two main groups: larger stores were designed to hold the bomb casings and high explosive components, and the small concrete huts to hold fissile cores. Quite bizarrely, the only personnel permanently stationed at the base were



The Vulcan bomber. The bomb-bay (seen open) had to be redesigned to allow the aircraft space to carry the Blue Danube

BARNHAM

RAF Police officers responsible for guarding the base.

The kiosks appear randomly placed in the wood, but early aerial photos show they were logically positioned. Each kiosk is fronted by a steel encased wooden door, which, during its operational life, was fitted with a combination lock. Rusting radiation symbols are still visible on some of the doors, so too are electrical fittings inside and outside each kiosk. The doors had a large spring-loaded electrical contact, which sent a signal to the control building to indicate if the door was open or closed. Once inside, visitors will notice a hole or cavity in the solid concrete floor (some of the structures have two holes). The holes supported steel vessels to store the nuclear



A short walk through the main entrance reveals a huge watch tower and this puzzling construction



The huge hoist to remove the bomb from transporters is still evident. Behind is one of the buildings used to store the case

bunkers, they would believe Britain had more warheads than it actually did. Gently rising pathways once used to trolley materials into the kiosks are still visible. So too are the old-fashioned lamp posts that helped guide RAF personnel guard dog patrols at night.

The actual bomb was brought to the base on large transporters. Two huge heavy steel-framed structures and a 10 tonne hoist remain intact to this very day. The device lifted the explosive part of the bomb and casing into large non-nuclear storage buildings. Each storage unit measured about 60 x 20 yards and was divided into 11 bays long by three bays wide with two internal lines of supporting concrete pillars. The Blue Danube bomb



Two bomb-blast walls still exist on the estate

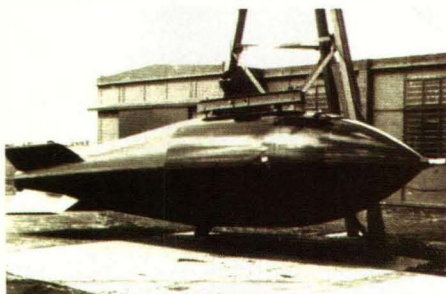
material. Forty eight single-hole stores, known as Type 'A' were constructed, these would have held a single plutonium core. The remainder, known as Type 'B' buildings would have held two cobalt cores. The kiosks were connected via a path system. At some point during the operational life of RAF Barnham, the holes of Type 'B' huts were filled in and covered by gritless asphalt.

Cold War Deception

Some experts believe part of Barnham's role was also one of deception, in that if the Russians noted dozens of nuclear storage



Once away from the roadside, visitors find themselves in a wooded area, and though most of the paths are overgrown, it's not long before the outline of dozens of small structures hidden by trees become visible



Blue Danube

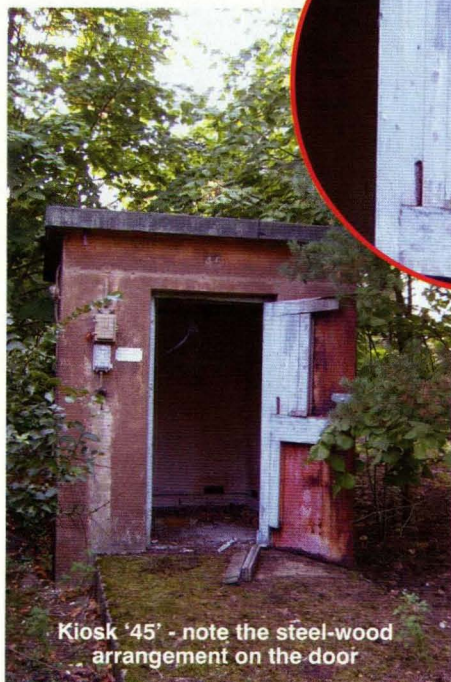
measured 24ft 2in and had a diameter of 5ft 2in and weighed 10,000lbs. Its enormous length and the maintenance required (and the fact that it was free-falling) rendered it almost useless before its service career (1957-1961) had even begun. Blue Danube's fins extended after being dropped so that it could be carried inside the bomb bays of Britain's V-bombers - Valiant, Vulcan and Victor. Just how many bombs were stored at RAF Barnham is unclear, though Britain had an arsenal of just 20 Blue Danubes so it's evident the facility was operating well below its capacity.

The bombs were stored without their fissile components in three almost identical buildings joined by an internal loop road. One of the warehouses was damaged by fire in the 1980s and was demolished. However, the other two remain.

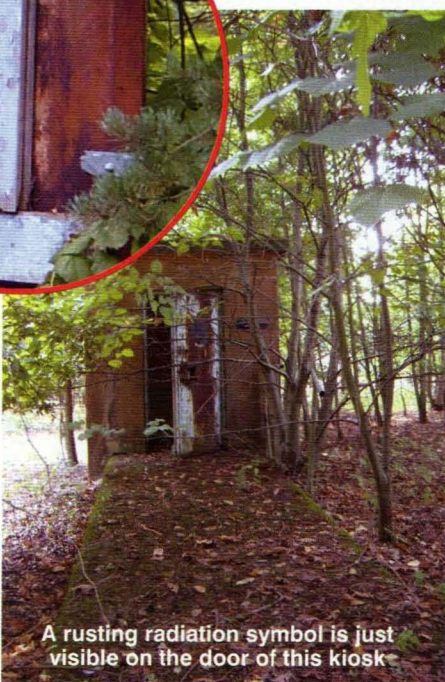
Rusting metal fence posts and rails that guided base staff to the H-block positioned huts still protrude from the grass. From above, the bomb store and boundary plan are barely visible due to the trees. The base was encompassed with an inner and outer fence and a concrete wall added a third line of protection. Dog patrols were constant between the fences and quite often the animals would be allowed to roam freely.



Some buildings are now occupied by small firms - but the evidence of Barnham's past is all around - including these interesting rail/trolley tracks



Kiosk '45' - note the steel-wood arrangement on the door



A rusting radiation symbol is just visible on the door of this kiosk

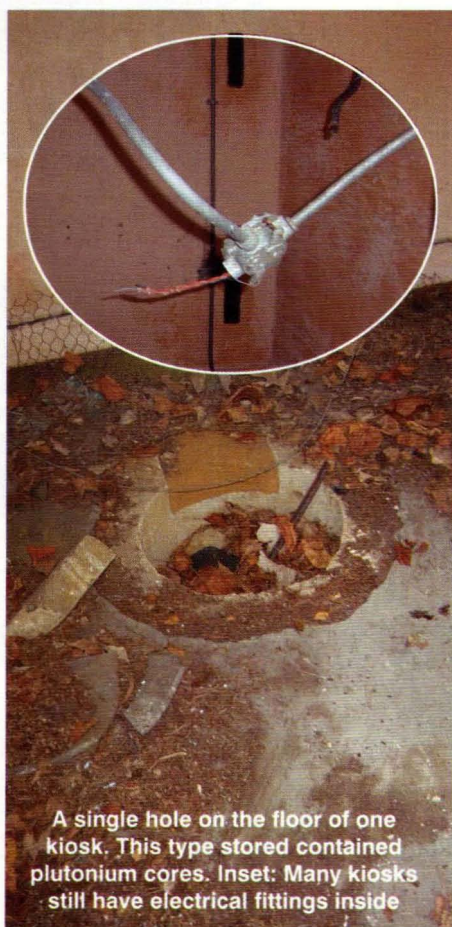


Nature has made the roof of this kiosk invisible from the air - or was it intentional?

Giant watch towers built in 1959 to augment security still exist. The towers were positioned in a manner to monitor all sides of the base and helped keep intruders out. Indeed, to our knowledge there was only ever one breach of security during RAF Barnham's nuclear history. One tower is in extraordinarily good condition and affords an excellent view of the base. Also still visible are train or trolley tracks used to move materials across the base.

RAF Barnham's nuclear role was short lived. By 1960 military specialists regarded such weapons (dropped by bombers) as obsolete. They were superseded (as the principal British nuclear deterrent) by the stand off missile Blue Steel, and the storage and maintenance of nuclear weapons moved to other RAF bases. It's believed the last nuclear bomb was removed from RAF Barnham in 1963 and the site sold to its present owner. Another storage facility virtually identical to Barnham was built at Faldingworth in Lincolnshire.

The manager gave Eye Spy a guided tour around this most impressive site. Readers who may be interested in visiting the estate should always seek his permission before entering. RAF Barnham is just a short drive from the town of Thetford. Please note that the MOD still uses adjoining land. National Grid Reference TL 8517 7988



A single hole on the floor of one kiosk. This type stored contained plutonium cores. Inset: Many kiosks still have electrical fittings inside

QUALITY EYE SPY BINDERS



Order Ref: ES/099

UK £7.50
USA \$17.00
ROW £9.50 -
price includes P & P

Please use order form on page 82



Keep your magazines in pristine condition with Eye Spy's smart binders - each binder holds eight editions



WITH SUBSCRIPTION CARD UK £6.50 USA \$15.00 ROW £8.50

EYE SPY INTELLIGENCE MAGAZINE SUBSCRIPTION CARD



EYE SPY
INTELLIGENCE MAGAZINE

SUBSCRIPTION CARD

valid until subscription expires - non-transferable

Peter Davison SUBSCRIPTION NO. 201206214

Telephone UK 01756 770199
USA 877 309 9243
e-mail eyespy@eyespyimag.com



A subscription to Eye Spy Intelligence Magazine is already excellent value, but its now even better. From 1 November 2006, all subscribers will receive a subscription card and a unique number that enables readers to claim discount on a wide variety of purchases, including books, videos, trade equipment and much more. Wherever you see the card (as above - binder

advert) discounts will be available. Similarly, we are negotiating with other companies who will recognise the card and act accordingly. The card remains valid throughout the subscription period. When ordering any item, simply add your number - it's that easy.

• Existing subscribers can send a SAE to Eye Spy to receive their card, or simply wait until the subscription is renewed.



EYE SPY TRADE BOOKS 200

INTELLIGENCE MAGAZINE

EYE SPY SPECIALIST BOOKS AND MANUALS FOR ALL ASPECTS OF... INTELLIGENCE • ESPIONAGE • SECURITY
• SURVEILLANCE • SAFETY • DETECTION • EQUIPMENT • FORENSICS • COUNTERSURVEILLANCE • MILITARY TRAINING

For detailed information on these and many more titles go to www.eyespy.com

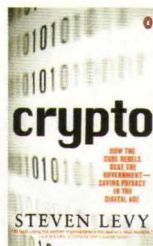
All prices shpwm include postage and packing • Includes air mail delivery to USA, Europe and Rest of World

Use order form on page 82 - or go to www.eyespy.com or telephone direct

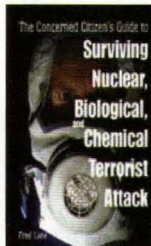
www.eyespy.com
FOR OUR FULL SELECTION
OF TRADE BOOKS



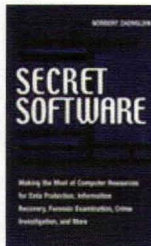
FBI GUIDE TO CONCEALABLE WEAPONS
FBI GUIDE to concealable weapons. Packed with photos. Softback 86pp
E\$966 \$18.00 \$25.00



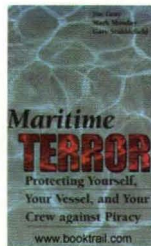
CRYPTO Code rebels. Humble the hackers and spooks. Essential. Paperback 352pp
E\$903 \$10.00 \$20.00



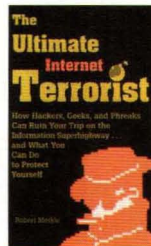
CITIZEN'S GUIDE Surviving nuclear, biological, chemical attacks. Softback 80pp
E\$866 \$17.00 \$22.50



SECRET SOFTWARE Data, forensics, crime investigation. Softback 128pp
E\$861 \$20.00 \$38.00



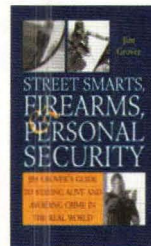
MARITIME TERROR Protection against piracy. Softback 72pp
E\$869 \$14.50 \$30.50



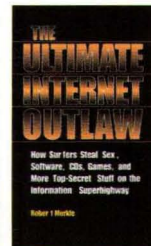
ULTIMATE INTERNET TERRORIST The dangers revealed. Softback 152pp
E\$1041 \$18.00 \$36.00



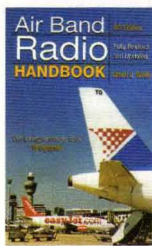
UBERHACKER II MORE WAYS TO BREAK INTO A COMPUTER Softback 370pp
E\$1039 \$39.95 \$68.00



STREET SMARTS, FIREARMS, AND PERSONAL SECURITY Guide to Staying Alive. Softback 280pp
E\$1111 \$28.00 \$45.00



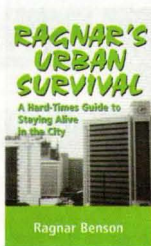
ULTIMATE INTERNET OUTLAW Softback 96pp
E\$1040 \$15.00 \$29.00



AIR BAND RADIO HANDBOOK 2005 For the enthusiast and professional alike. Softback 208pp
E\$971 \$14.99 \$30.00



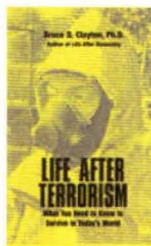
US ARMY SPECIAL FORCES MEDICAL HANDBOOK Softback 608pp
E\$1094 \$30.50 \$35.00



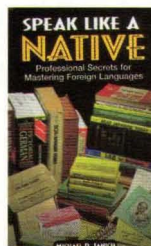
RAGNAR'S URBAN SURVIVAL Staying alive in the city. Softback 200pp
E\$1097 \$20.00 \$25.00



RUNNING A RING OF SPIES Spy craft and black operations in real world of espionage. Softback 216pp
E\$860 \$25.00 \$48.00



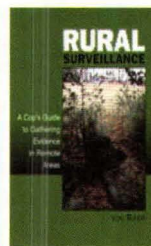
LIFE AFTER TERRORISM What you need to know to survive today. Softback 192pp
E\$868 \$21.50 \$40.00



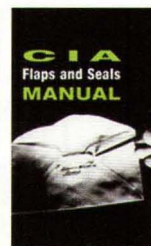
SPEAK LIKE A NATIVE Professional secrets for mastering languages. Softback 192pp
E\$961 \$20.00 \$30.00



THE ULTIMATE SCANNER The complete guide to scanning. Large Softback 242pp
E\$963 \$34.99 \$48.00



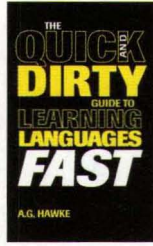
RURAL SURVEILLANCE Police guide to gathering evidence in remote areas. Softback 128pp
E\$881 \$22.00 \$40.00



CIA FLAPS AND SEALS MANUAL Learn the art of opening letters and packages. 56pp
E\$1147 \$13.99 \$16.00



WORKING IN A WAR ZONE Cashing in safely after the shooting stops. Softback 184pp
E\$875 \$17.50 \$34.00



QUICK AND DIRTY GUIDE TO LEARNING LANGUAGES FAST Softback 176pp
E\$1018 \$20.00 \$37.99



ADVANCED SURVEILLANCE Complete Manual of Surveillance Training. Softback 400pp
E\$712 \$24.99 \$40.00



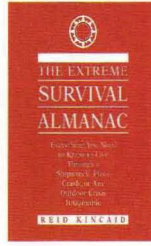
WHO ARE YOU? The encyclopedia of personal identification. Softback 352pp
E\$1006 \$26.95 \$50.00



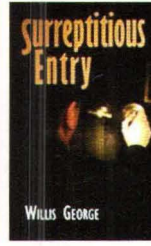
SECRETS OF STREET SURVIVAL Staying alive in a civilian warzone. Softback 400pp
E\$809 \$29.99 \$50.00



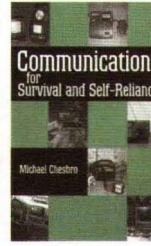
DON'T BUG ME The Latest High-Tech Spy Methods. Softback 152pp
E\$1005 \$22.95 \$45.00



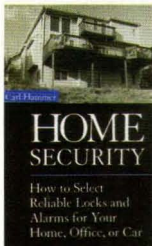
EXTREME SURVIVAL ALMANAC Everything you need to know. Softback 480pp
E\$1093 \$50.00 \$56.00



SURREPTITIOUS ENTRY Government breaking and entering operations. Softback 208pp
E\$1151 \$25.00 \$30.00



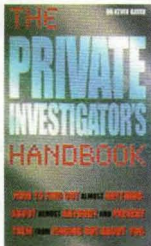
COMMUNICATIONS FOR SURVIVAL AND SELF-RELIANCE Softback 216pp
E\$1096 \$30.00 \$35.00



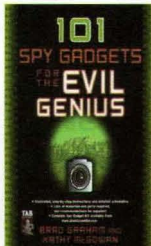
HOME SECURITY How to select locks and alarms for your home/business. Softback 128pp
E\$988 \$22.99 \$32.00



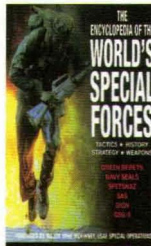
STOPPING SUICIDE ATTACKERS Secrets of an Israeli counterterrorist. Softback 128pp
E\$865 \$20.00 \$38.50



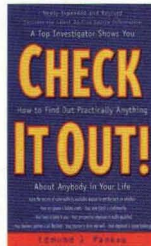
PRIVATE INVESTIGATOR'S HANDBOOK How to find out anything on anybody. 192pp
E\$813 \$9.99 \$25.00



101 SPY GADGETS Build your own spy equipment. Softback 259pp
E\$1183 \$18.00 \$38.00



WORLD'S SPECIAL FORCES Encyclopedia of special forces, air, sea, land. Hardback 255pp
E\$886 \$28.00 \$55.00



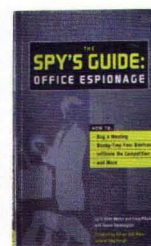
CHECK IT OUT How to find out practically anything. Softback 160pp
E\$1074 \$19.00 \$28.00



PRACTICAL MARTIAL ARTS FOR SPECIAL FORCES How to use your hands. Softcover, 112pp
E\$1091 \$18.00 \$24.00



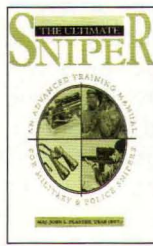
DO IT YOURSELF MEDICINE How to find and use the most effective drugs. Softback 128pp
E\$1095 \$20.00 \$23.00



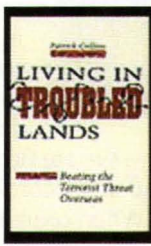
THE SPY'S GUIDE: OFFICE ESPIONAGE Professional tips. Softback 170pp
E\$722 \$12.00 \$20.00



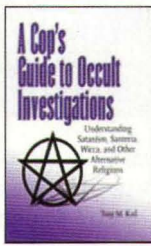
DIGITAL PRIVACY A guide to computer security. Essential tips. Softback
E\$1003 \$25.00 \$50.00



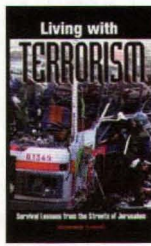
THE ULTIMATE SNIPER Advanced training for military and police. Huge Softback 543pp
E\$965 \$50.00 \$70.00



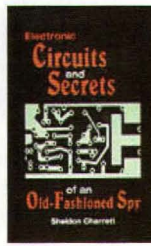
LIVING IN TROUBLED LANDS Beating the Terrorist Threat Overseas. Softcover 192pp
E\$1113 \$21.00 \$35.00



COP'S GUIDE TO OCCULT INVESTIGATIONS A police must. Softback 184pp
E\$1043 \$25.00 \$29.00



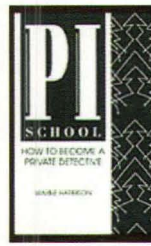
LIVING WITH TERRORISM Survival Lessons From the Streets of Jerusalem. Softback
E\$1116 \$19.00 \$30.00



ELECTRONIC CIRCUITS AND SECRETS old-fashioned spy - bugs and more. Softback 128pp
E\$908 \$22.99 \$40.00



SCANNER MODIFICATIONS AND ANTENNAS Modifying equipment. Softback 176pp
E\$910 \$18.00 \$35.00



PI SCHOOL: HOW TO BE A PRIVATE INVESTIGATOR Softback 112pp
E\$1072 \$19.00 \$25.00



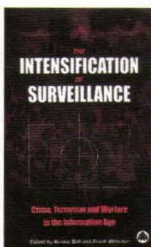
HOW TO HIDE ANYTHING Learn how to construct dozens of hiding places. Softback 120pp
E\$1117 \$16.00 \$26.00



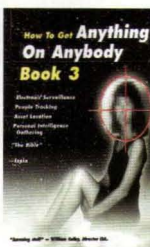
TACTICAL TRACKING OPERATIONS
The Essential Guide for Military and Police Trackers
Softback 170pp
£8827 \$38.00 \$60.00



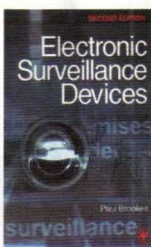
INVISIBLE ADVANTAGE
Ghille suit construction made simple
Softback 80pp
£9114 \$13.99 \$25.00



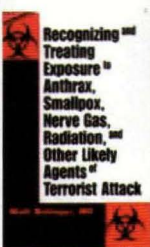
THE INTENSIFICATION OF SURVEILLANCE
Crime, terrorism and warfare
Softback 176pp
£8825 \$25.00 \$45.00



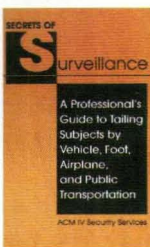
HOW TO GET ANYTHING ON ANYBODY
Special Security Work
Massive Softback
£5737 \$65.00 \$109.00



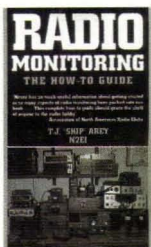
ELECTRONIC SURVEILLANCE DEVICES
Microphones, transmitters etc.
Softback 112pp
£8807 \$24.99 \$45.00



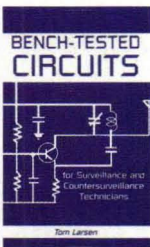
RECOGNIZING AND TREATING EXPOSURE
Anthrax, smallpox, nerve gas, radiation, Softback 112pp
£8870 \$17.00 \$23.50



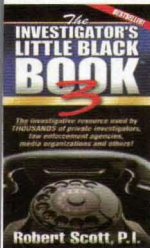
SECRETS OF SURVEILLANCE
A Professional's Guide to Tailing Subjects by Vehicle, Foot, Airplane, and Public Transportation
Softback 176pp
£8814 \$29.99 \$50.00



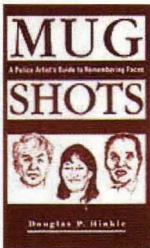
RADIO MONITORING
The 'know how guide' packed with tips
Softback 176pp
£964 \$25.00 \$35.00



BENCH-TESTED CIRCUITS
For countersurveillance technicians
Softback 128pp
£8824 \$15.00 \$32.00



INVESTIGATOR'S LITTLE BLACK BOOK
Major US-based resource guide
Softback 504pp
£8806 \$19.99 \$35.00



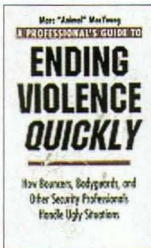
MUG SHOTS
A police detective guide to remembering faces
Softback 128pp
£8880 \$20.00 \$38.00



BUG BOOK Everything you wanted to know about electronic eavesdropping
Softback 168pp
£907 \$30.50 \$50.00



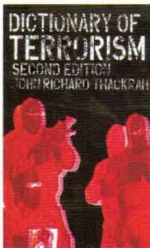
SPY GAME Winning through super technology
Huge Softback 520pp
£8862 \$35.00 \$60.00



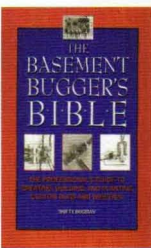
ENDING VIOLENCE QUICKLY Avoid injuries and law suits - professional guide
Softback 256pp
£8894 \$21.99 \$40.00



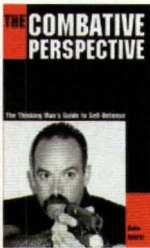
EXECUTIVE PROTECTION A professional's guide to bodyguarding
Softback 112pp
£8872 \$15.50 \$31.00



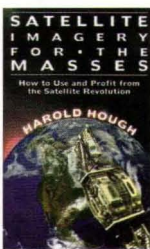
DICTIONARY OF TERRORISM Every group, individual listed. Essential
Softback 448pp
£9975 \$25.00 \$48.00



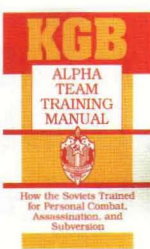
THE BASEMENT BUGGER'S BIBLE Everything you need to know about bugs
Softback 312pp
£947 \$34.99 \$60.00



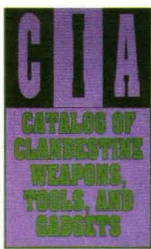
COMBAT PERSPECTIVES The thinking man's guide to self-defence
Softback 112pp
£8884 \$17.50 \$34.00



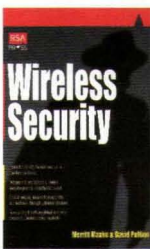
SATELLITE IMAGERY FOR THE MASSES
How to use and profit from satellite photos
Large Softback 200pp
£81169 \$28.00 \$29.99



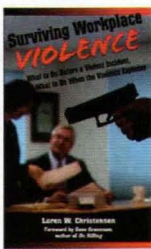
KGB ALPHA TEAM TRAINING MANUAL
Combat, assassination and subversion
320pp
£8808 \$24.99 \$45.00



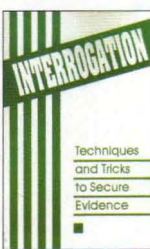
CIA CATALOG Clandestine weapons, tools and gadgets
Softback 128pp
£944 \$18.00 \$28.00



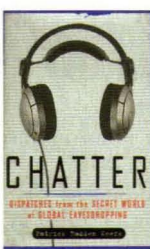
WIRELESS SECURITY Professional tips to secure your wireless network
Softback 300pp
£980 \$25.00 \$49.99



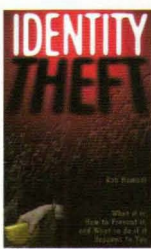
SURVIVING WORKPLACE VIOLENCE What to do, and how to act
Softback 120pp
£81017 \$19.99 \$20.00



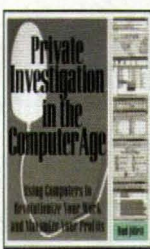
INTERROGATION RCMP guide, techniques and tricks to secure evidence
Softback 88pp
£811 \$19.50 \$38.00



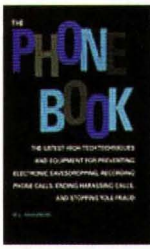
CHATTER Conversations from the secret world of eavesdropping
Hardback 300pp
£950 \$25.00 \$35.00



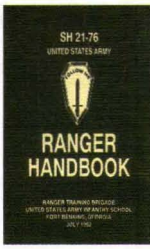
IDENTITY THEFT Secrets of counter identity theft and protecting yourself
Softback 241pp
£950 \$12.99 \$25.00



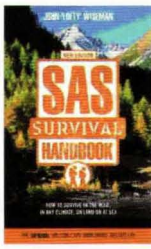
PRIVATE INVESTIGATION IN THE COMPUTER AGE Using computers
Softback 176pp
£8859 \$25.50 \$50.00



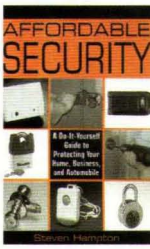
THE PHONE BOOK Stop eavesdroppers, telephone bugs, phone call fraud and more
Softback 280pp
£8858 \$30.00 \$60.00



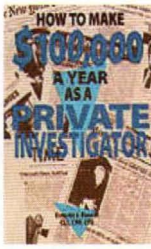
RANGER HANDBOOK US Army Ranger. Rare small manual.
Softback 448pp
£8810 \$26.00 \$48.00



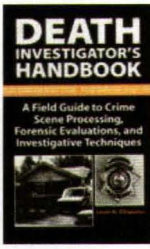
SAS SURVIVAL HANDBOOK Survive in any climate, land or sea.
Softback 576pp
£8830 \$24.00 \$45.00



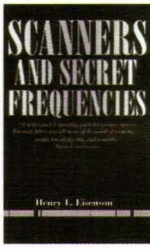
AFFORDABLE SECURITY Survive in any climate, land or sea.
Huge Softback 888pp
£8830 \$24.00 \$45.00



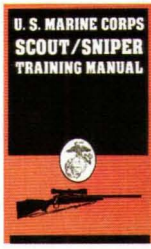
HOW TO MAKE \$100,000 A YEAR AS A PRIVATE INVESTIGATOR
Investigator
Softback 128pp
£8857 \$21.50 \$40.00



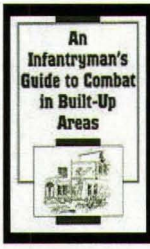
DEATH INVESTIGATOR'S HANDBOOK Field guide to crime scene forensics.
Massive Hardback 888pp
£8879 \$75.00 \$100.00



SCANNERS AND SECRET FREQUENCIES All you need to know.
Softback 314pp
£9567 \$25.00 \$38.00



U.S. MARINE CORPS SCOUT/SNIPER TRAINING MANUAL Product of US Marine Corps
Softback 576pp
£9599 \$29.99 \$40.00



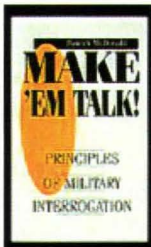
COMBAT IN URBAN AREAS Ground operations in urban settings.
Softback 312pp
£8888 \$29.99 \$58.00



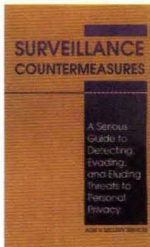
KILL OR GET KILLED Longest-selling book on close combat in history.
Softback 420pp
£8889 \$45.99 \$80.00



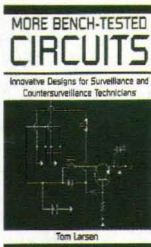
THE WHOLE SPY CATALOG Everything you need to know about espionage.
Softback 448pp
£8886 \$35.00 \$55.00



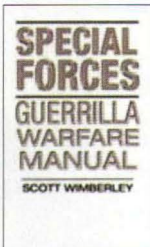
MAKE 'EM TALK! Principles of military interrogation. Professional guide.
Softback 80pp
£8890 \$17.99 \$35.00



SURVEILLANCE COUNTERMEASURES Detecting, evading and enduring threats.
180pp
£8835 \$29.99 \$48.00



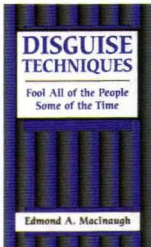
MORE BENCH-TESTED CIRCUITS Innovative designs for surveillance and countersurveillance technicians
Softback 72pp
£8909 \$19.99 \$38.00



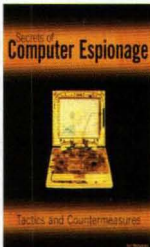
SPECIAL FORCES Guerrilla warfare manual for successful operations.
Softback 248pp
£912 \$22.99 \$42.00



SOE SECRET OPERATIONS All the secrets of how the SOE and OSS used spy craft in WWII
272pp
£1150 \$25.00 \$25.00



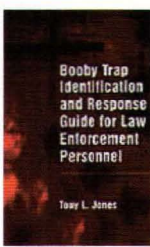
DISGUISE TECHNIQUES Fool all of the people some of the time.
Softback 82pp
£962 \$18.00 \$28.00



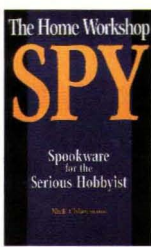
SECRETS OF COMPUTER ESPIONAGE Tactics and countermeasures.
Softback
£8790 \$25.00 \$46.00



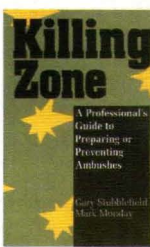
THE EXTREME COVERT CATALOG - SPECIAL TRADE SECURITY IMPORTED
Massive Softback
£8738 \$50.00 \$60.00



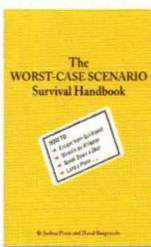
BOOBY TRAP IDENTIFICATION Response guide for law enforcement personnel.
Softback 80pp
£8876 \$20.00 \$38.00



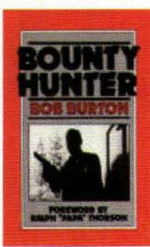
HOME WORKSHOP SPY Spookware for the serious hobbyist.
Softback 104pp
£8856 \$24.50 \$48.00



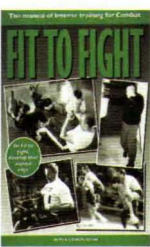
KILLING ZONE A professional's guide to preventing ambushes.
Softback 240pp
£960 \$25.00 \$40.00



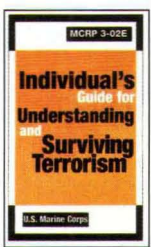
WORST-CASE SCENARIO TRAVEL Survival handbook
Softback 192pp
£8805 \$12.00 \$24.00



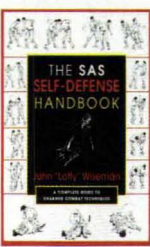
BOUNTY HUNTER Professional guide to the art of bounty hunting.
Softback 136pp
£8873 \$15.50 \$30.00



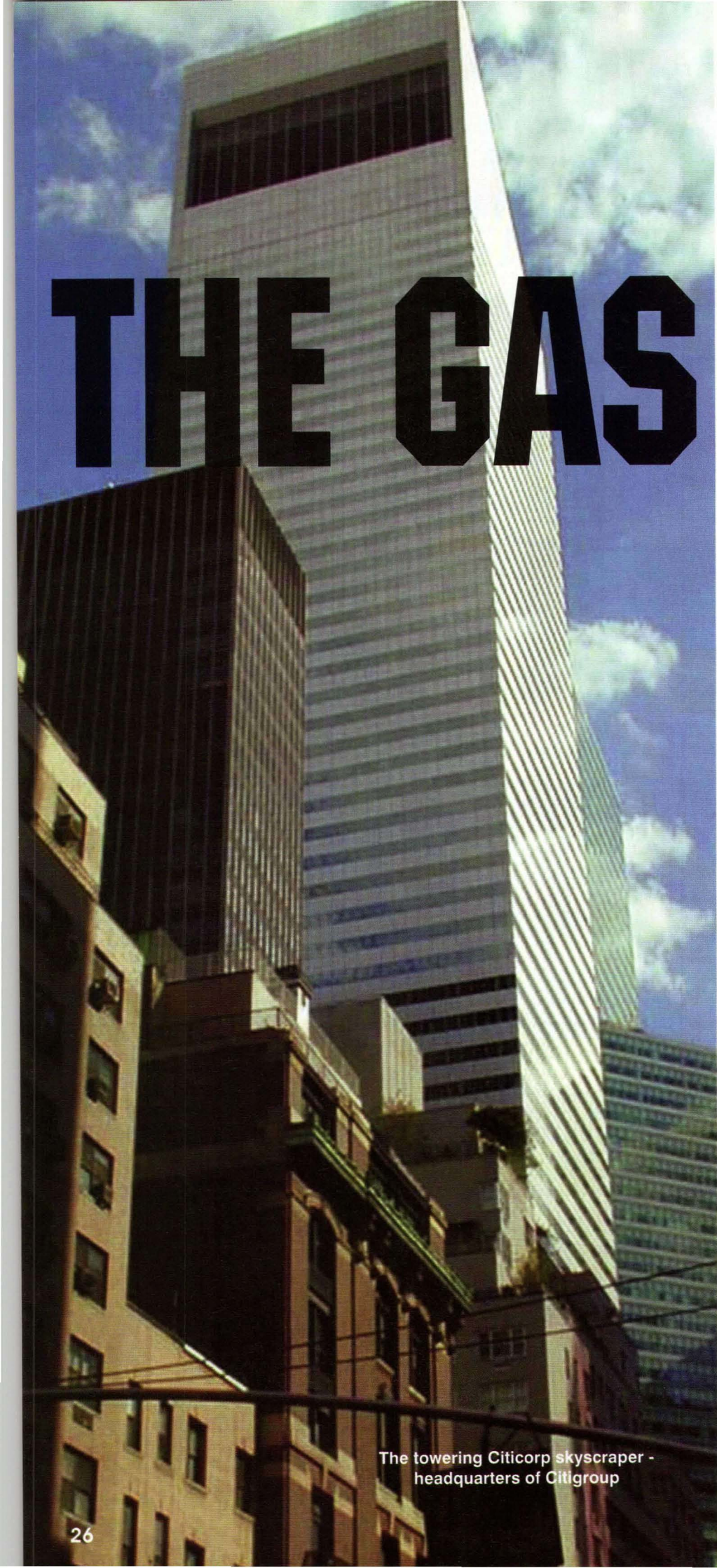
FIT TO FIGHT Complete manual of intense training for combat.
Softback 183pp
£654 \$18.00 \$30.00



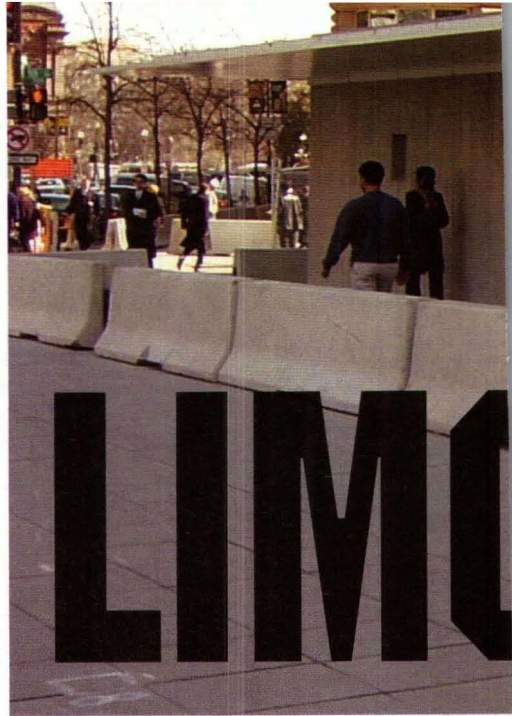
SURVIVING TERRORISM Packed with essential tips and advice.
Softback 86pp
£971 \$12.50 \$18.00



SAS SELF-DEFENSE HANDBOOK Complete guide to unarmed combat.
Softback 240pp
£8831 \$29.99 \$48.00



THE GAS



LIMOS

**IN 2004, AL-QAIDA'S
BRILLIANT CODEMAKER
WAS ARRESTED...**

**INFORMATION FOUND ON
HIS COMPUTER LED
POLICE TO LONDON AND
THE DEADLY
'GAS LIMOS PROJECT'**

On 12 October 2006, Dhiren Barat admitted planning for a series of attacks against key buildings and locations in an operation he himself dubbed 'The Gas Limos Project'. Barat also pleaded guilty to charges that he intended to cause mayhem by exploding a radioactive 'dirty bomb' and three vehicles packed with explosives in underground car parks. MI5 regard his arrest as one of the most significant ever in the fight against terrorism.

Seven other men are to stand trial in connection with the plot next April. They all deny conspiracy to murder and commit public nuisance with radioactive materials, toxic gases, chemicals or explosives. One of the men faces charges under the Terrorism Act in connection with an alleged plot to target financial institutions in the United States.

The towering Citicorp skyscraper -
headquarters of Citigroup

THE WORLD BANK GROUP

S PROJECT



NYPD Hercules police officer.
Above: The World Bank in Washington DC - another target analysed by Barat

stone [main target] of a series of planned attacks'.

Barot intended to hire three limousines and pack them with propane gas cylinders and explosives. The vehicles would then be driven into underground car parks directly underneath highly populated buildings. The locations were not specified in court, but all were in the UK.



New York Stock Exchange area

According to intelligence sources, this defendant is said to have possessed detailed plans of the Prudential Building in Newark, New Jersey that could help a person committing or preparing an act of terrorism.

13 JULY 2004 - ARREST OF THE CODEMAKER

In Eye Spy 28 (August 2004) we reported upon the arrest of al-Qaida operative Moham-

med Naeen Noor Khan at Lohare Airport by security officials of Pakistan's Inter Service Intelligence agency (ISI). His demise began weeks earlier after he had attached a cell phone to 18 pounds of explosives on a busy Karachi road. The device failed to detonate. Police traced one of the phone numbers stored in the phone to an address in the city. The ISI raided the apartment and found Mussad Aruchi, Khan's nephew and the son of a well known al-Qaida liaison man. GCHQ and the NSA began tracking other telephone numbers, but at the time, both organisations had no idea who Khan was or the significance of what they were about to discover. Khan was eventually traced and kept under surveillance. He was arrested at the airport as he attempted to collect a parcel. Unbeknown to the ISI, Khan was an al-Qaida operative given the nickname 'The CodeMaker'.

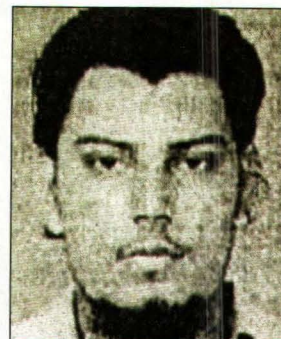
At the time of his arrest Khan was carrying a laptop computer. Two other computers at an address used by Khan and 50 CD-Roms were seized. These contained the names of dozens of operatives and hundreds of contacts who were regarded as 'safe' and willing to help al-Qaida's cause. Within days of Khan's arrest, MI5 raided several locations and detained Barot and other suspects in and around London. MI5 analysts discovered plans to bring down the huge Citicorp building in New York; attack financial institutions such as the World Bank in Washington DC, and render the area around the New York Stock Exchange totally useless because of the radiation fallout from a dirty bomb. Another target was the International Monetary Fund (IMF) headquarters in Washington. Several operations were written down in notebooks. One was headed 'Rough Presentation for Gas Limos Project'. Another note said [this is] *the main corner-*



Prudential Building, Newark

AL-QAIDA SURVEILLANCE

Main entrance to the Citigroup Center building in Manhattan. Eye Spy understands the terrorists believed its unique design made it vulnerable



**Mohammed Naeen
Noor Khan**

Eye Spy learned of the plot two years ago (see Eye Spy 28) but Barot's guilty plea has meant further details being released. The vehicle based bombs may or may not have resulted in the destruction of

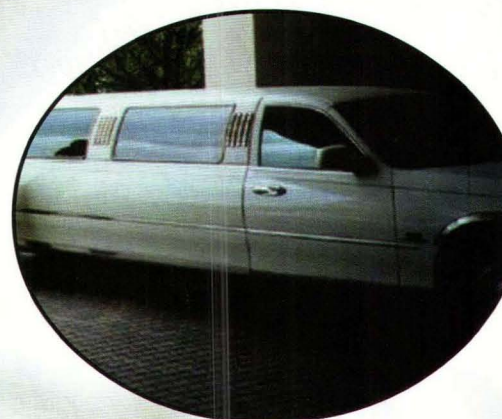
the Citicorp building, but its strange design has often been criticised by security officials. Following the discovery of Barot's computer, MI5 immediately notified law enforcement officials in New York and Washington. NYPD then launched a major surveillance operation after intelligence suggested the building had been under observance from US-based suspects from a nearby cafe. Our exclusive photographs show a member of NYPD's Hercules operation guarding the Citicorp building on the day intelligence was forwarded to New York officials in 2004.

© JAY GOLDBERG NEW YORK

August 2004: An NYPD officer guards the Citicorp building following MI5 operations in London

According to Eye Spy sources the following questions relating to surveillance on the buildings in the USA were asked by Khan. The data was retrieved from a computer

- Is the building occupied by undercover or uniformed security guards?
- What are the daily routines or shift-patterns of the guards?
- Are traffic lights situated near or in front of the building - these offer a stopping point for a truck bomb, for example?
- What explosives are required to generate heat above 2,700F (1,480C)?
- Has the building a weak-point or additional protection against explosives?
- How soon could security and emergency forces reach the scene?
- Where are the nearest police and fire stations situated?
- Where are the security cameras fixed - and are there cameras on approach to the area?
- Does the building have an underground car park?
- Where are the exit points?
- Are crash barriers situated around the building?
- Where are the delivery and service points to the building located?



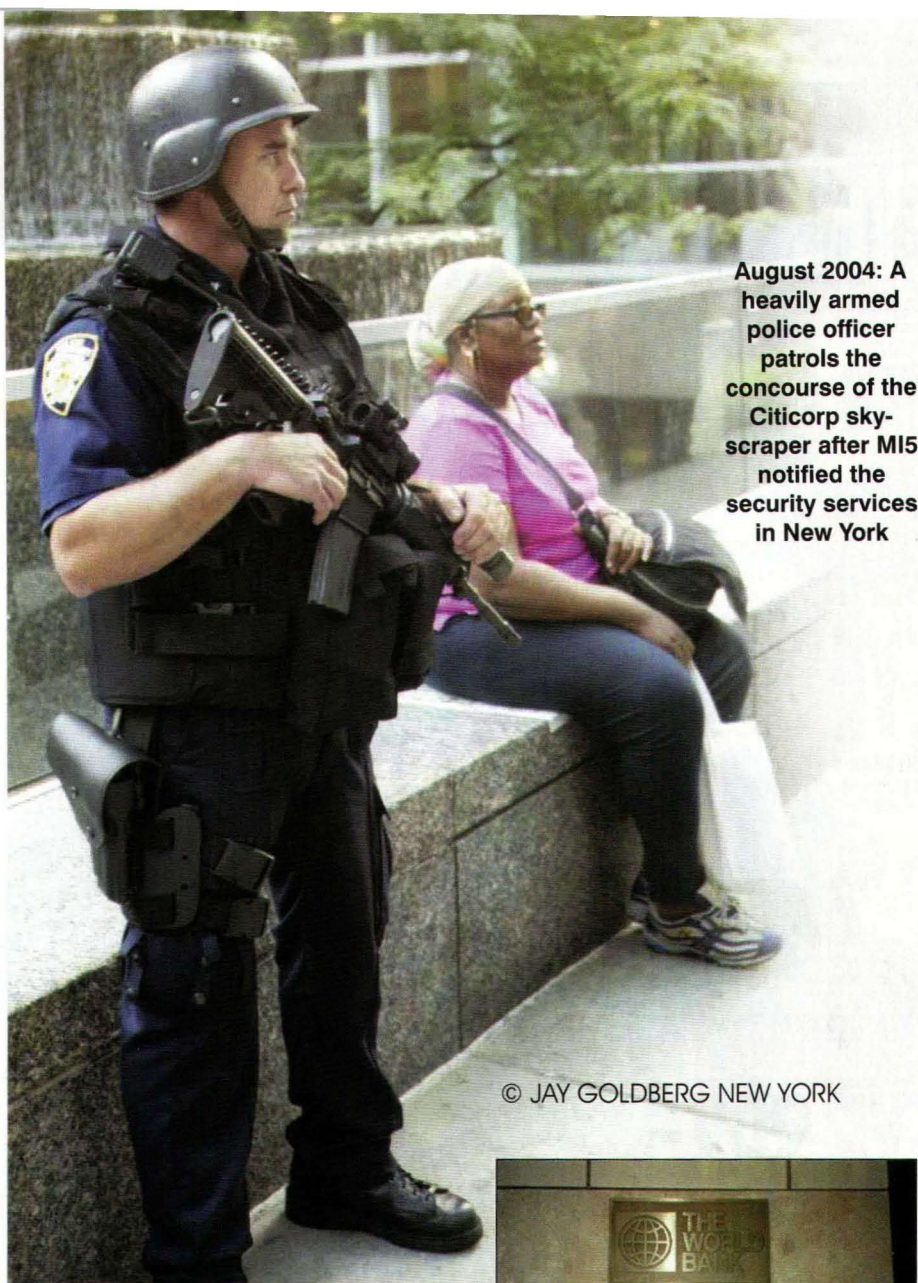
Barot's planning was meticulous. Following the limousine explosions, he admitted that he intended to detonate a "synchronised" dirty bomb explosion. That location is still unknown, though Eye Spy sources believe it was the New York Stock Exchange area in Lower Manhattan. Experts agree the bomb itself would not have caused many (if any) casualties immediately, but hundreds of people would have been contaminated and suffered radiation sickness at a later date. Similarly, the result would have caused panic throughout many global financial institutions. The Wall Street locale is one of the most heavily secured areas of New York and has undergone various security alterations in the last two years, including high-visibility patrols, CCTV cameras, and is patrolled regularly by specialist NYPD officers.

Woolwich Crown Court heard that Barot, 34, from Willesden, northwest London, would not have warned the authorities that bombs were in place. He simply wanted "to kill as many innocent people as possible."



Left: Badat probably decided to use Limousines as they are hugely popular in many major cities and are spacious.

Though they attract attention they are rarely challenged by police and most underground car parks can accommodate their size



August 2004: A heavily armed police officer patrols the concourse of the Citicorp skyscraper after MI5 notified the security services in New York

© JAY GOLDBERG NEW YORK



In court Barot looked relaxed and took notes on his laptop computer. He entered a plea of guilty to the first count on an indictment containing 23 charges, including a "conspiracy to commit murder conducted between January 2000 and his arrest in August 2004." Edmund Lawson, QC, for the prosecution, said Barot had admitted planning terrorist murders in the US and Britain.

Mr Lawson said: "The principal planned attack involved packing three limousines with gas cylinders and explosives then detonating the devices in underground car parks."

As for the dirty bomb plot, Mr Lawson noted that this would have caused "fear, panic and social disruption." Mr Lawson also revealed: "The parts of the conspiracy relating to the United States are contained in plans found by the police on computers after his arrest."

MI5 and Scotland Yard found no evidence whatsoever that the Gas Limos Project had received financial backing, and no bombmaking equipment or vehicles had been

physically acquired. The plot existed only on paper and in the mind of Barot.

Mr Lawson ended by telling the court: "They were plans to carry out explosions at all those premises with no warning, plainly designed to kill as many innocent people as possible."

Mr Lawson said that by admitting his own guilt Barot, "makes no admission with regard to the involvement of any of his seven co-defendants in the conspiracy."

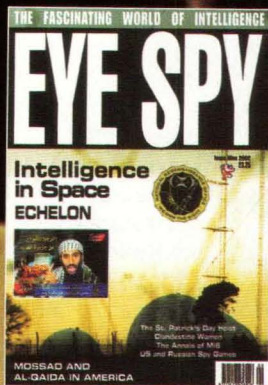
The case against seven other men arrested in raids involving anti-terrorist officer in 2004, will take place in 2007. The men deny all allegations against them.

Editor's note: Eye Spy 28 carries a major feature on the arrest of Khan, and details of his work. Khan visited the UK on six occasions.

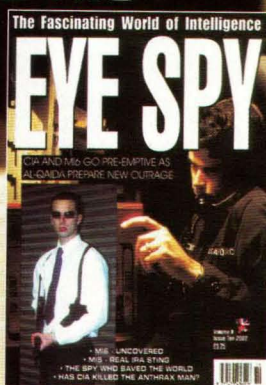
VOLUME TWO

VOLUME THREE

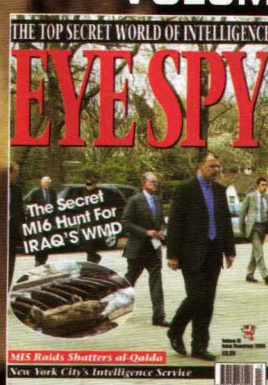
VOLUME FOUR



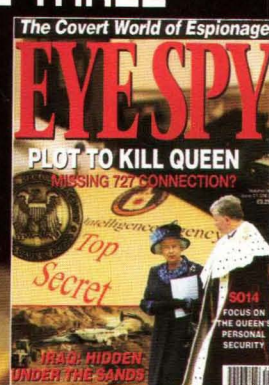
ISSUE 9 REF: ES/09
USA \$7.00 UK £3.50 EUR €4.50



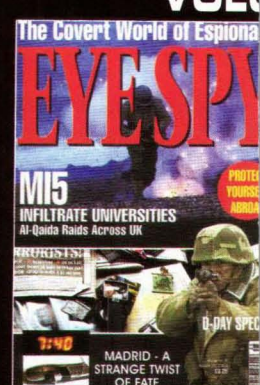
ISSUE 10 REF: ES/10
USA \$7.00 UK £3.50 EUR €4.50



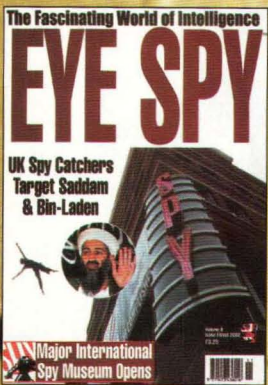
ISSUE 17 REF: ES/17
USA \$7.00 UK £3.50 EUR €4.50



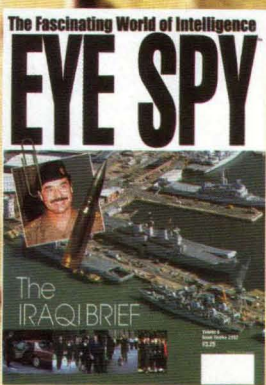
ISSUE 21 REF: ES/21
USA \$7.00 UK £3.50 EUR €4.50



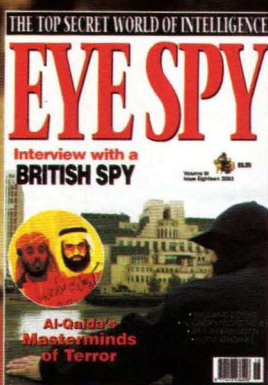
ISSUE 25 REF: ES/25
USA \$7.00 UK £3.50 EUR €4.50



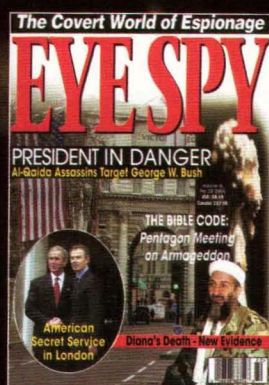
ISSUE 11 REF: ES/11
USA \$7.00 UK £3.50 EUR €4.50



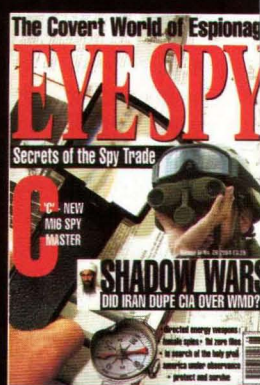
ISSUE 12 REF: ES/12
USA \$7.00 UK £3.50 EUR €4.50



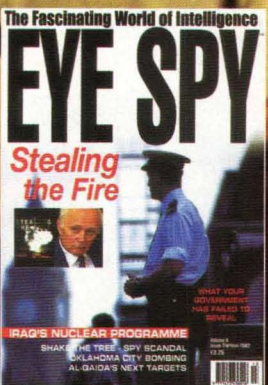
ISSUE 18 REF: ES/18
USA \$7.00 UK £3.50 EUR €4.50



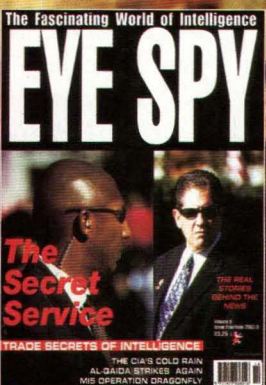
ISSUE 22 REF: ES/22
USA \$7.00 UK £3.50 EUR €4.50



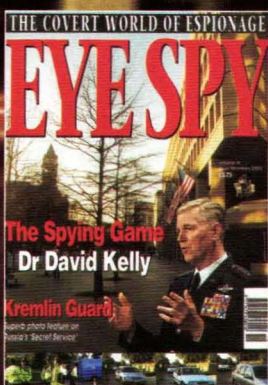
ISSUE 26 REF: ES/26
USA \$7.00 UK £3.50 EUR €4.50



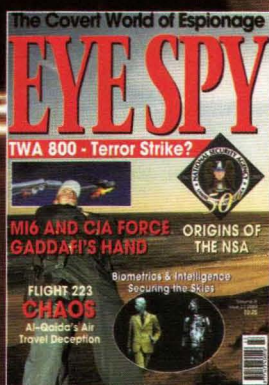
ISSUE 13 REF: ES/13
USA \$7.00 UK £3.50 EUR €4.50



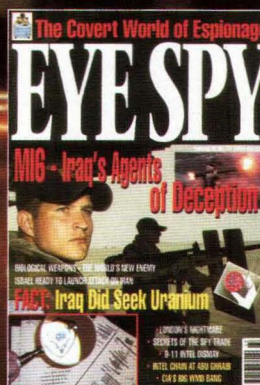
Issue 14 Ref: ES/14
USA \$7.00 UK £3.50 EUR €4.50



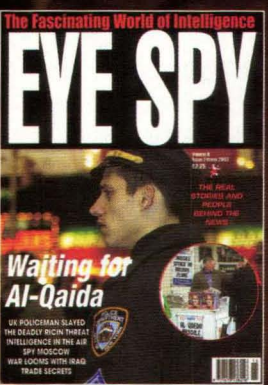
ISSUE 19 REF: ES/19
USA \$7.00 UK £3.50 EUR €4.50



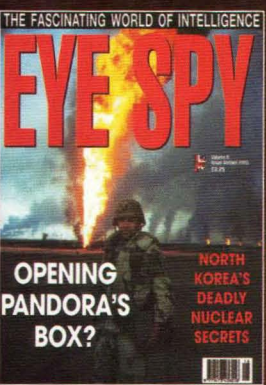
ISSUE 23 REF: ES/23
USA \$7.00 UK £3.50 EUR €4.50



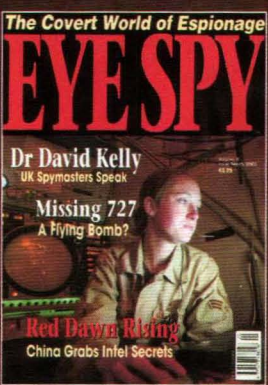
ISSUE 27 REF: ES/27
USA \$7.00 UK £3.50 EUR €4.50



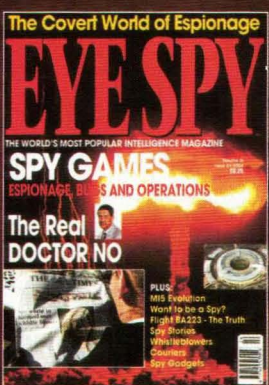
ISSUE 15 REF: ES/15
USA \$7.00 UK £3.50 EUR €4.50



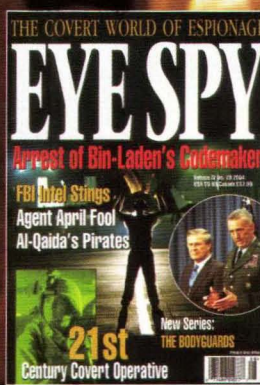
ISSUE 16 REF: ES/16
USA \$7.00 UK £3.50 EUR €4.50



ISSUE 20 REF: ES/20
USA \$7.00 UK £3.50 EUR €4.50



ISSUE 24 REF: ES/24
USA \$7.00 UK £3.50 EUR €4.50



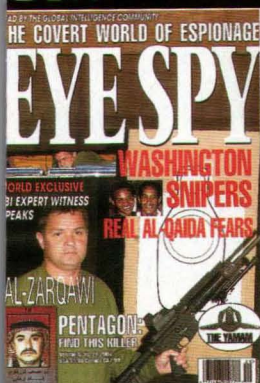
ISSUE 28 REF: ES/28
USA \$7.00 UK £3.50 EUR €4.50

Each highly collectable edition represents a worldwide overview of global intelligence

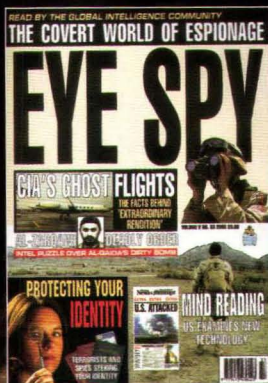
OUR

VOLUME FIVE

VOLUME SIX



ISSUE 29 REF: ES/29
USA \$7.00 UK £3.50 EUR €4.50



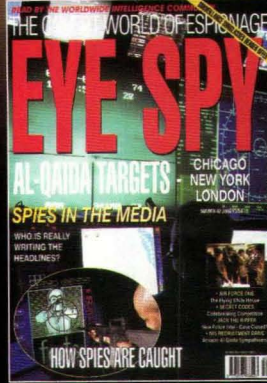
ISSUE 33 REF: ES/33
USA \$7.00 UK £3.50 EUR €4.50



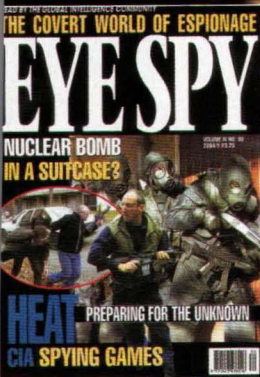
ISSUE 34 REF: ES/34
USA \$7.00 UK £3.50 EUR €4.50



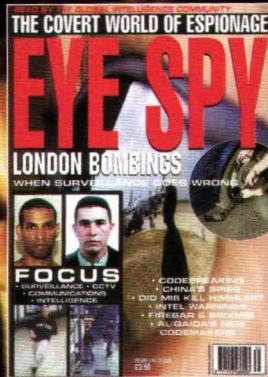
ISSUE 41 REF: ES/41
USA \$7.00 UK £3.50 EUR €4.50



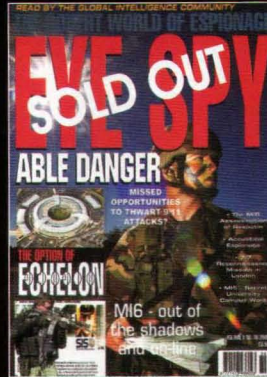
ISSUE 42 REF: ES/42
USA \$7.00 UK £3.50 EUR €4.50



ISSUE 30 REF: ES/30
USA \$7.00 UK £3.50 EUR €4.50



ISSUE 35 REF: ES/35
USA \$7.00 UK £3.50 EUR €4.50



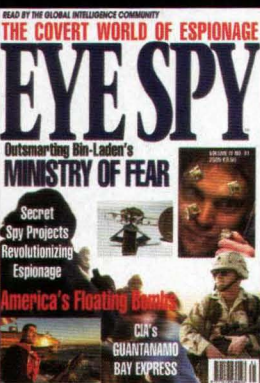
ISSUE 36 REF: ES/36
USA \$7.00 UK £3.50 EUR €4.50



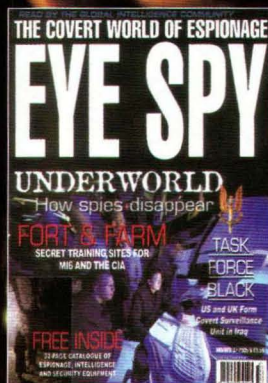
ISSUE 43 REF: ES/43
USA \$7.00 UK £3.50 EUR €4.50

**SAVE MONEY -
BUY IN VOLUMES
WITH EYE SPY'S
LUXURY BINDER!**

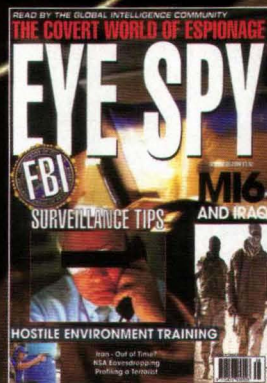
See pages 60-61 for details



ISSUE 31 REF: ES/31
USA \$7.00 UK £3.50 EUR €4.50



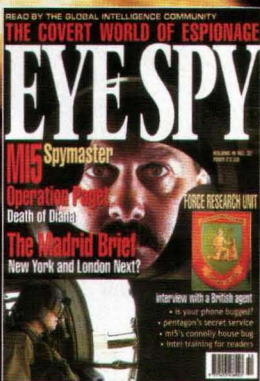
ISSUE 37 REF: ES/37
USA \$7.00 UK £3.50 EUR €4.50



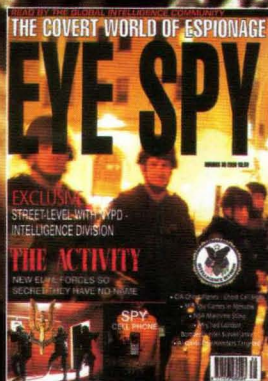
ISSUE 38 REF: ES/38
USA \$7.00 UK £3.50 EUR €4.50

**STILL AVAILABLE FROM
VOLUME ONE**

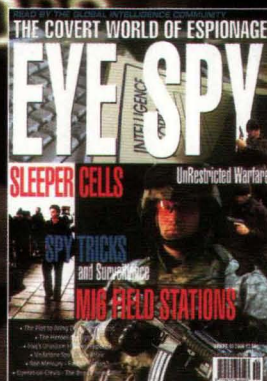
ISSUE 2 REF: ES/02 USA \$7.00 UK £3.50 EUR €4.50	ISSUE 4 REF: ES/04 USA \$7.00 UK £3.50 EUR €4.50	ISSUE 8 REF: ES/08 USA \$7.00 UK £3.50 EUR €4.50
---	---	---



ISSUE 32 REF: ES/32
USA \$7.00 UK £3.50 EUR €4.50



ISSUE 39 REF: ES/39
USA \$7.00 UK £3.50 EUR €4.50



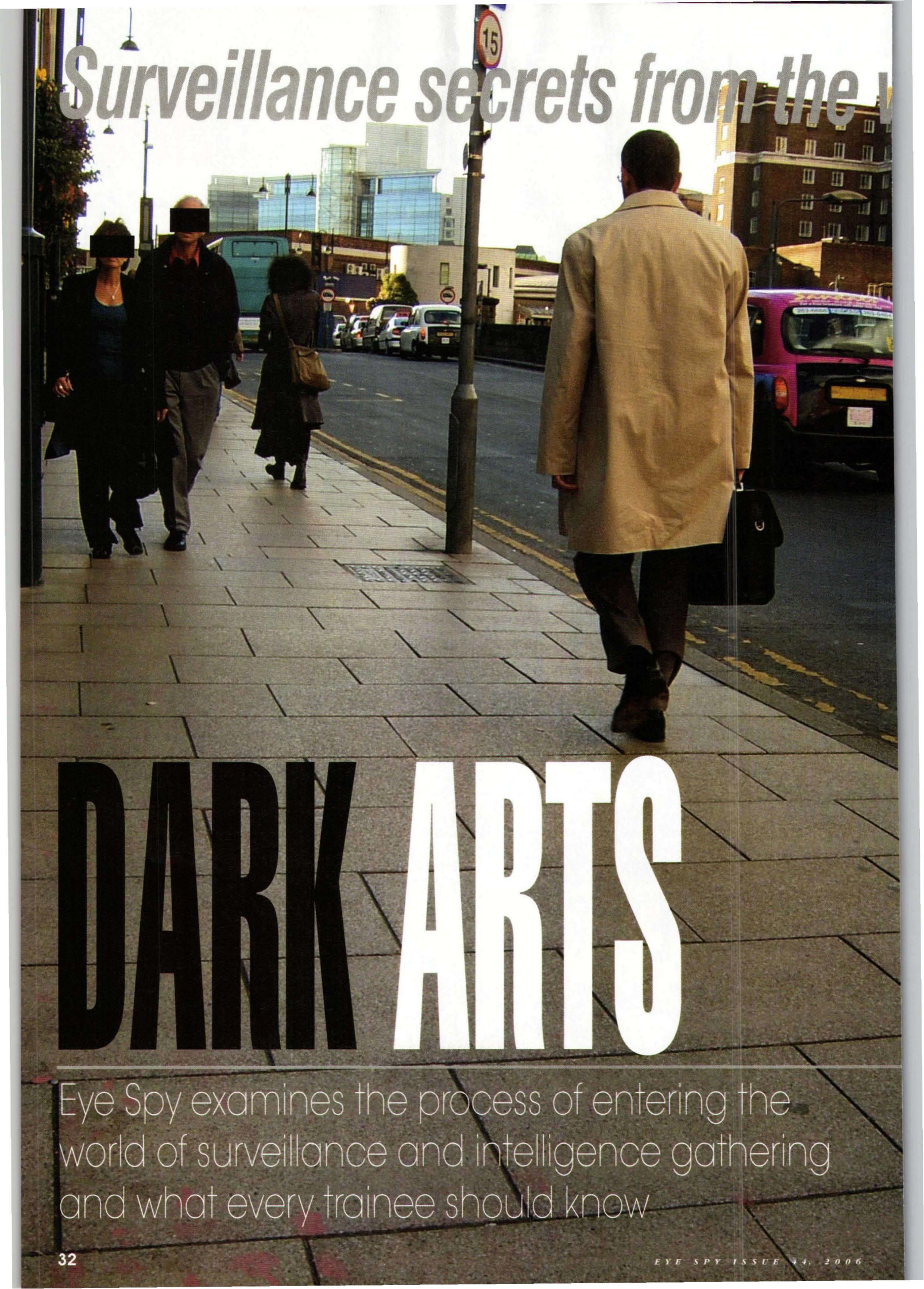
ISSUE 40 REF: ES/40
USA \$7.00 UK £3.50 EUR €4.50

EYE SPY BACK ISSUES
ORDER FROM UK OR NEW YORK
(SEE PAGE 82)
OR ON-LINE www.eyespymag.com

ORDER BY PHONE:
UK, EUROPE AND REST OF WORLD
TELEPHONE: 01756 770199 (UK)

NORTH AMERICAN READERS
TOLL FREE: 877 309 9243

events - your bridge to the covert world of espionage and intelligence



Surveillance secrets from the

DARK ARTS

Eye Spy examines the process of entering the world of surveillance and intelligence gathering and what every trainee should know

World's leading security services

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 be 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.

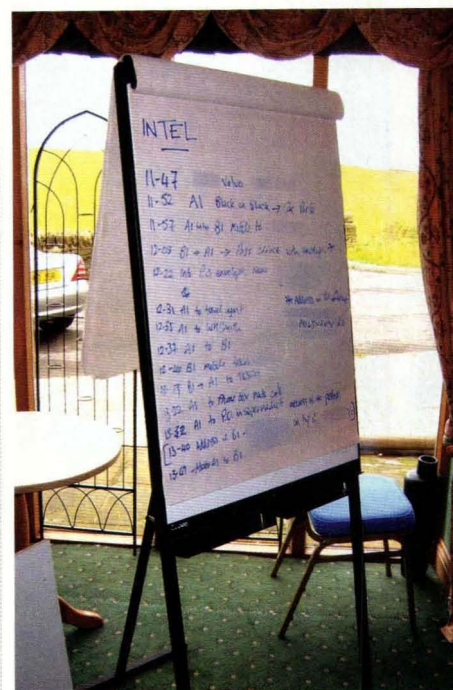
Questions relating to fitness, eyesight and hearing are obvious. But what of the trainee's observational skills, or acting ability - essential in 'acting normally' in ordinary, unusual or difficult situations? Training in the use of surveillance equipment is also necessary, so too is knowing how to wear 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 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 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 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 (a feature on disguise techniques is scheduled for Eye Spy 45).

RULES

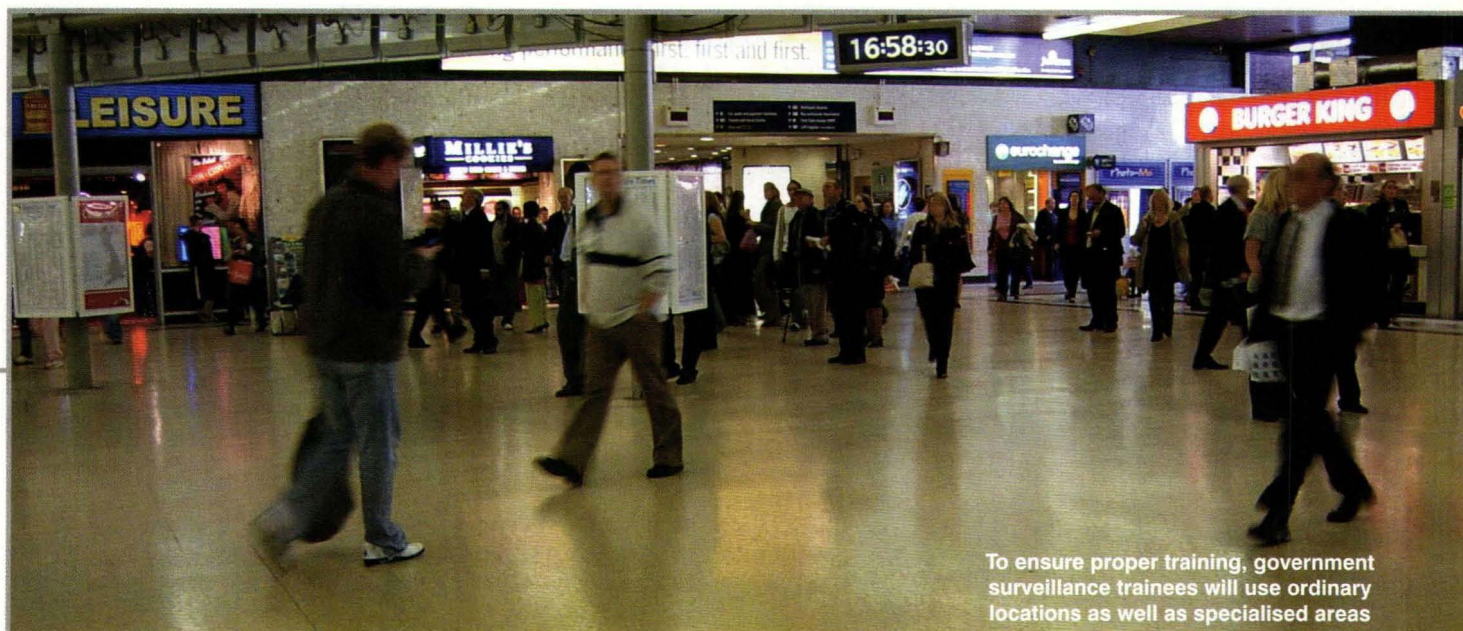
Coloured hair, wearing bright clothes or brilliant designer shirts with recognisable logos, white



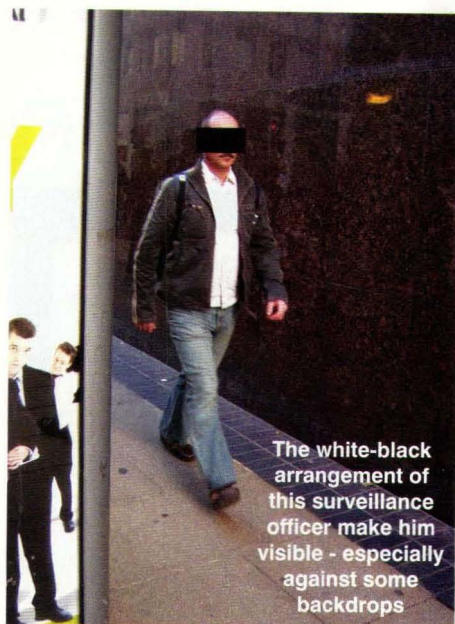
A surveillance debrief board identifying times and relevant intelligence

trainers or red T-shirts, jewellery etc. is simply not acceptable, unless of course, the officer intends to visit a night club or similar. Long hair is problematic in some cases, but it can always be tied up, or cut. If future operations demand, operatives can always regrow their hair.

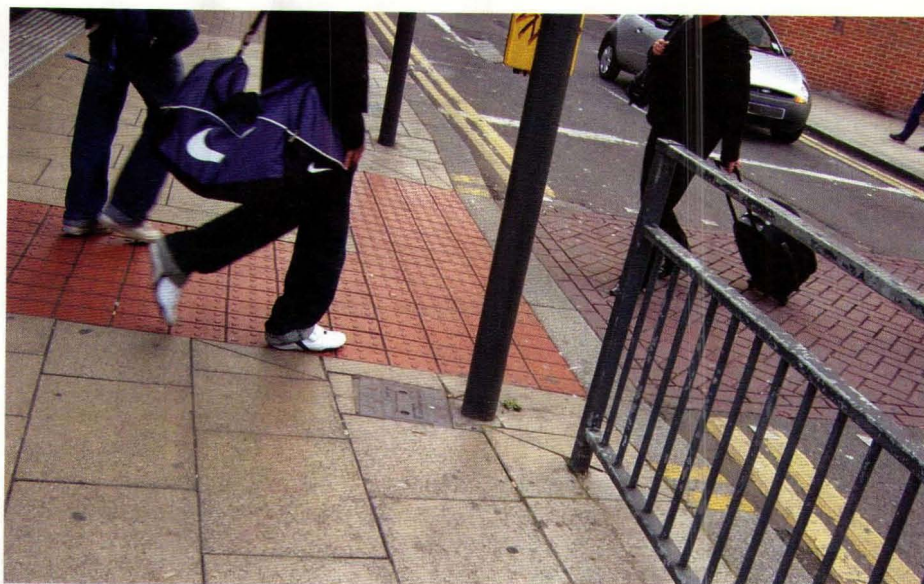
Dress sense is crucial in that the operative appears normal in a crowd or location and does not attract undue attention. Even if the target he is shadowing notices him, two, three or four times, it's unlikely he will remember every detail. But these odds go down if he remembers a logo, a gold chain or bright boots. During a night-time



To ensure proper training, government surveillance trainees will use ordinary locations as well as specialised areas



The white-black arrangement of this surveillance officer make him visible - especially against some backdrops



White sport shoes, though comfortable for walking, are to be avoided

surveillance operation, operatives will always don dark clothing, but trainees are warned - some clothes do 'shine' and reflect under certain lighting conditions. They are told to avoid anything white - or a white-black arrangement. Analysis of clothing and cloth, head-wear and footwear in various conditions is an important part of surveillance training.

WEATHER CONDITIONS

Trainees are taught to examine weather conditions, especially prior to an operation. If it is going to rain or snow, a coat or jacket are useful additions, lest the officer is the only one walking up and down the street absolutely soaked. If it doesn't rain, this garment can always be removed, dumped and collected later (it's not wise to carry this garment under the arm for hours it may be noticed). A plastic carrier is always a useful addition - a removed coat or jacket can quickly be placed in the bag. Selecting the correct footwear is important, especially in adverse weather. These are obvious codes of conduct, but some trainees still have to be told - "Don't walk into a rock concert wearing a suit - it simply won't work - and don't walk into a business environment wearing jeans." Any inadvertent breach of codes will be noticed by trainers or senior officers, and may jeopardise the future prospects of a trainee.

In later training exercises, MI5 surveillance operatives are shown how to wear or carry 'additional garments under existing sets of clothing' and are skilled in the removal or application of such. Specially designed clothing is also available such as reversible jackets, sweaters and head wear.

STREET WISE, ESSENTIALS AND TRICKS

Once on the street, trainees are advised against changing their appearance too much. It's helpful to carry one or two additional items. A couple of hats, spectacles (clear glass), a second jacket etc. Wearing items that might make an operative

appear threatening, aggressive or "shifty" are to be avoided. Sunglasses are fine if everyone else is wearing them - but not at midnight. If the exercise involves visiting a library, carrying a book might prove useful. Surveillance officers will use anything to help maintain their invisibility and conceal the deception.

Cash is an essential asset. There are times when a surveillance operative will be required to follow a target into a shop, cafe, bar, amusement arcade, turf accountant (betting shop) etc., or occasionally purchase a travel ticket, hop onto a bus, hail a taxi or even make a phone call. Standing about in a betting shop for an hour simply reading the odds will most certainly be viewed as 'odd'. Similarly, the target may go into a cafe to meet someone and be there for quite a while. Hanging about on a street corner for any length of time will attract undue attention from a passing police officer or member of the public. It only induces suspicion. A surveillance officer is trained to casually enter such an establishments purchase a drink and monitor. In most cases officers will refrain from buying a hot drink - it looks unusual to all concerned if he buys a hot cup of tea and then has to depart seconds later if the target leaves. A small cold drink can be consumed in seconds. However, if it's minus 10

'Acting normally' is an aspect drilled time and time again into the student

and freezing it could look unusual if he orders a chilled beer. Experienced officers will assess the situation and act accordingly.

ACTING AND OBSERVATION

An MI5 surveillance trainee will undergo various observation tests. A film may be played showing an everyday street scene. Several questions relevant to its content will be asked. Initially responses may be poor and diverse, but in time experience is developed and these skills can be taken on to the street. Making notes or even using a recorder is acceptable - even in a classroom environment. This is vital training and habit forming. It's important that all intelligence gleaned, time, location, actions etc. are recorded in a real surveillance. At the end of any operation, the intelligence is pooled and entered into a working log book. This becomes a treasure trove of information and provides analysts and senior officers with essential data.



There are few exceptions to the rule in respect of wearing bright clothing. However, in some situations - such as a surveillance at a pop concert or casual nightclub - they will probably go unnoticed



All professional surveillance officers are required to be able to use equipment

Acting normally throughout a surveillance operation is mandatory. Ducking and diving into alleyways and doors just because the target turns around could jeopardize the operation. Trainees are taught to ignore such actions and simply walk by the target. Eye contact is important at all stages of a surveillance - but when in close contact, it's better to not to look at the target. Nervous trainees may think their cover is blown, but in 99% of all cases the target has a genuine reason for turning back - and it's rarely because he wants to take a good look at the person following him. He could be about to cross the road, so he will stop at the kerbside, turn around and check for traffic. 'Acting normally' is an aspect drilled time and time again into the student. If he or she fails this part of the programme, there is virtually no need to proceed to the next test stage. If, however, the trainee genuinely feels their cover has been blown, they are taught to remove themselves from the scene. A senior officer will decide if further participation in the operation is possible.

In early training exercises, officers may initially partner a colleague, and then join a four or eight-man team. It's rare for an operative to work alone at the training stage. Most government surveillance operations involve multiple members (men and women), however, in the corporate world, it's not unusual to find operatives working by themselves. They may



Strange but true... female and male operatives acting as man and wife are often missed by those performing countermeasures

have been hired to monitor a target in a personal injury case or similar.

At MI5 and other counter-espionage or anti-terrorism units, a great deal of training actually takes place in the classroom or controlled environments. Using radios, understanding communications, driving methods, foot surveillance, photographic skills, and of course, knowing how to work as a team takes time. A parallel course in electronic surveillance helps trainees become familiar with a whole host of equipment, including microphones, cameras, transmitters etc. Similarly, knowing where to position yourself in a vehicle to obtain a good photograph or video clip of the target is a skill not easily taught. Yet by researching locations and testing these prior to an operation, the trainee will learn how to hide in plain sight and still manage to succeed.

In a busy street, for example, the target may be partially hidden by shoppers. It's advantageous that the operative stays on the outside of the pavement. This will, in most cases, afford a better view. If the street is empty, the officer is more exposed, thus it's preferable to stay close to buildings. This procedure means the operative can stop and view window displays or even enter shops if necessary to create a 'normal scene' in the event the target is becoming suspicious. Using shop windows or any reflective surface to augment surveillance is always helpful. However, the trainee is reminded that the target can also use this method - even inadvertently.

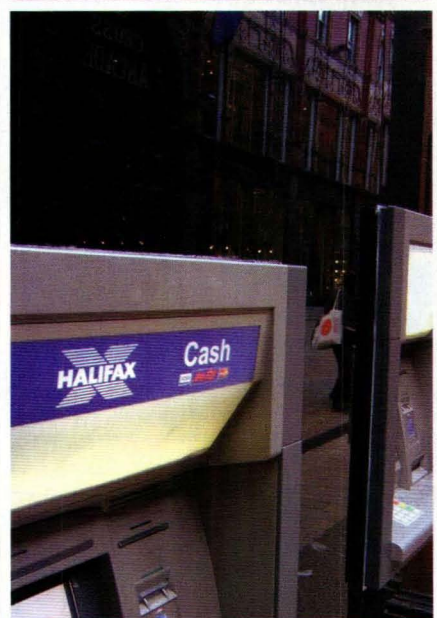
APPEARANCE

The trainee is given several subtle lessons in changing his or her appearance. However, disguise experts agree that this is a difficult area and can take a great deal of preparation - but it's necessary in some situations. If the officer stays covert and carries out the surveillance properly then using 'heavy' disguises should not be required. There are other methods that can be used that change the 'outline' of a person. The

UTILISING SURROUNDINGS



These images show two surveillance officers making imaginary phonecalls. However, in the above photo note the operative is utilising his surroundings, looks casual and has a wide field of vision. The officer below is isolated and looks decidedly uncomfortable and turns away

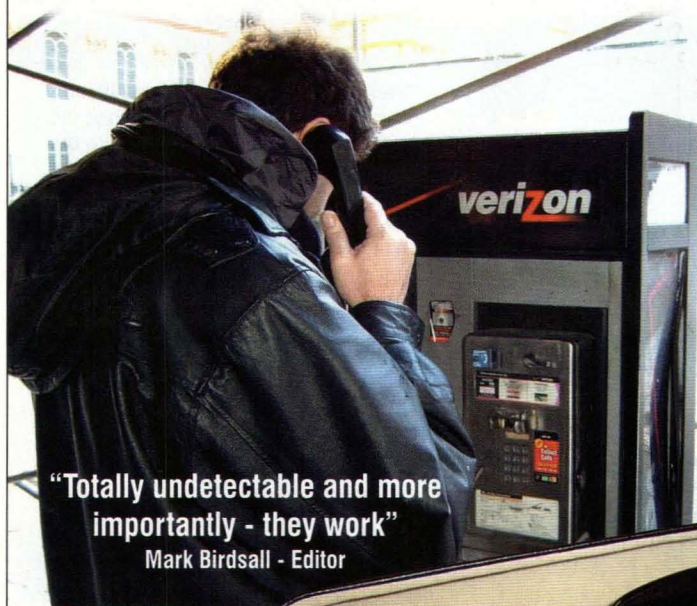


Stopping to use a cash machine is an ideal way to conceal a surveillance. In this case, the officer also uses a window to see the target's reflection

BEST-SELLERS WATCH YOUR BACK

EYE SPY'S HIGH-QUALITY REAR VISION SURVEILLANCE SUNGLASSES

Don't confuse these sunglasses with cheap toy models - interestingly, some may even bear the name 'Eye Spy'. Others still use plastic lenses and have mirrors attached to an extended (wide) frame. They are easily spotted. Our glasses have invisible and see-through reflective areas within the actual lens.



"Totally undetectable and more importantly - they work"

Mark Birdsall - Editor

Order code:
TX-RVS UK £30.00
USA \$35.00
ROW £35.00

SAVE MONEY!
See page 23 for details
of Eye Spy's new
SUBSCRIPTION CARD



Eye Spy Intelligence Magazine rear-vision surveillance sunglasses have a black-metal designer frame, rubber-backed ear drop-over (for comfort) and superb glass lenses. They also come in a tough smart black carry case.



WITH SUBSCRIPTION CARD UK £25.00 USA \$30.00 ROW £30.00



Please use order form on page 82 or call Eye Spy or visit www.eyespy.com



A dark alley providing an observation point is fine and the surveillance officer is totally invisible to the naked eye - but note what happens when someone decides to turn their living room light on

manner in which a person walks can be altered by using concealed splints behind the knee; wearing a knee bandage or placing a single shoe inlay will help induce a limp. Mastering disguise techniques is a vast subject, but the consensus of all professional surveillance trainers is "if you are going to do this - be dramatic".

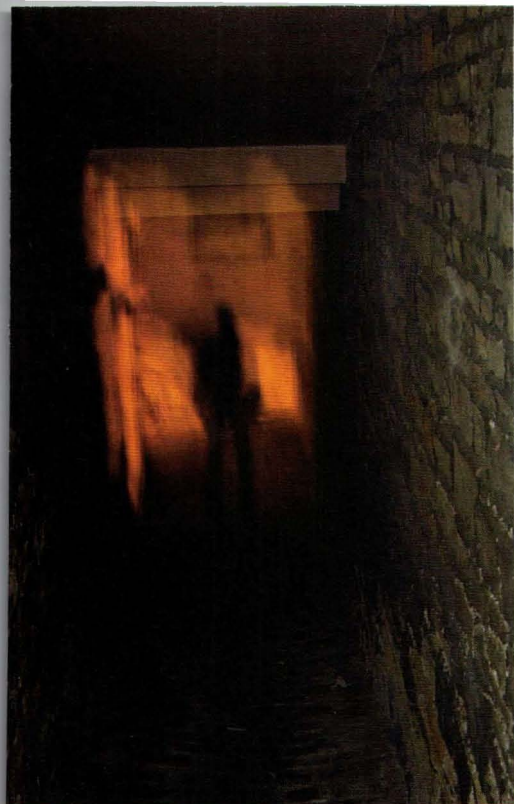
MORE TRICKS

Trainees are taught many tricks to conceal their role, including using everyday objects and situations such as withdrawing money from a cash machine, entering a telephone box or even lifting the bonnet of a car to suggest a breakdown. All these situations help provide cover.

Getting close to a target presents its own problems. For example, following the target into a railway station as he prepares to purchase a ticket. The trainee in this case, therefore, must stand immediately behind the target. It's likely he will overhear the target's intended destination as he buys a ticket. If that fails, he can always ask the seller "a ticket to the same place as my friend please." A little acting can go a long way.

The training is intense, but at some point trainees will test their skills in a carefully managed





exercise. The team may be given a briefing about a fictitious character or group and asked to gather as much intelligence as possible. In the scenario used here (based on an actual case), the primary target is a drugs dealer thought to have links with terrorism.

THE TEN POINT TEST

Armed only with a fuzzy photograph and the address of a bar/club where the target frequents, the team is asked to:

1. Locate the target's address
2. Obtain footage of the bar's interior
3. Identify locations for the installation of covert surveillance equipment
4. Identify and photograph colleagues and drug recipients
5. Note relevant vehicles
6. Discover the dealers methods in handling and forwarding cash
7. Determine who his primary agent is
8. Identify drugs' exchange locations
9. Recover receipts
10. Note cash transactions (depositing/ withdrawing money)



During the exercise, the trainers can monitor skill levels, note mistakes, point out good actions and act upon them accordingly. A training exercise provides instructors with an insight into the overall potential of each trainee. It's better to iron-out mistakes and problems at this stage rather than in a real-life situation.

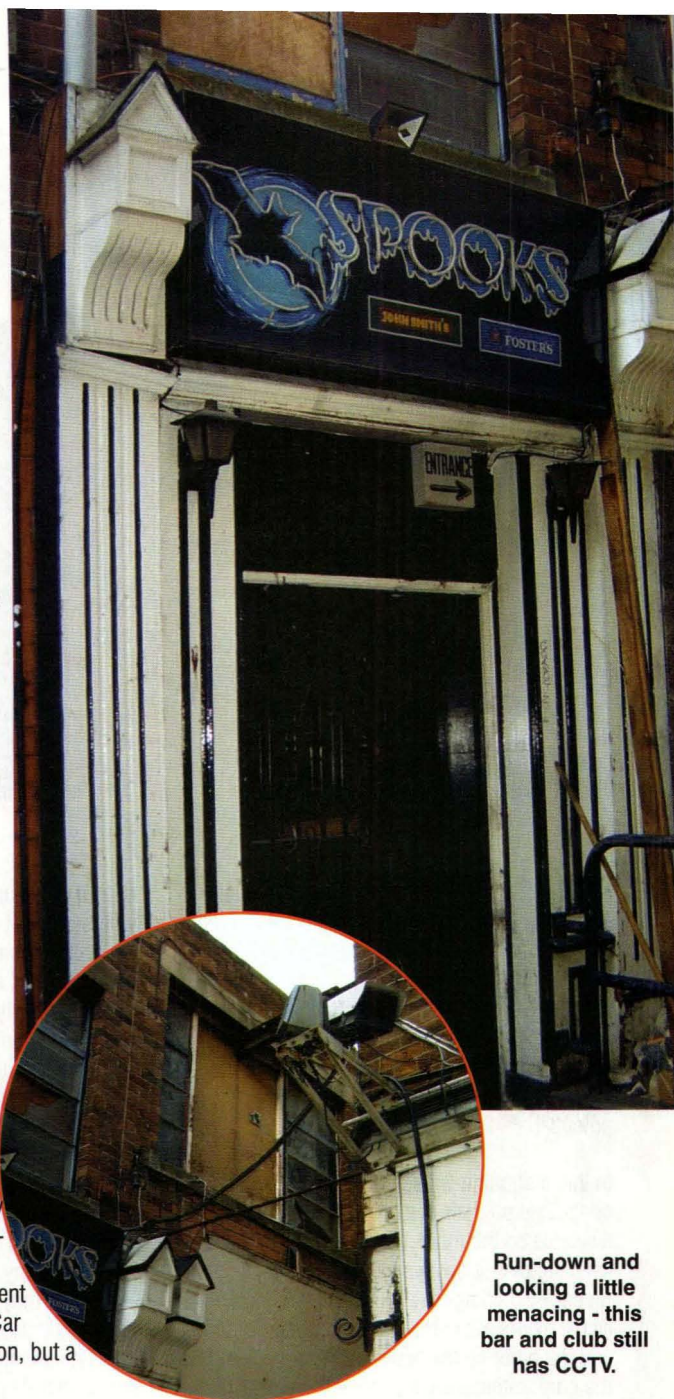
THE OPERATION

Preparation is a priority - briefings are frequent and always precede a surveillance. Trainees are invited to form teams, delegate roles and identify what equipment is necessary (including vehicles). Maps of the location, and a 'general surveillance area' must be identified. The operatives will research the bar, its clientele, drinks and food menu, opening and closing times, entry and exit doors, car parks, telephone boxes, study road maps, bus stops, taxi ranks and any transit points such as a nearby subway. Identifying a location that affords a covert monitoring point is also useful, lest the trainee is observed before the operation has even begun. The choice of vehicles is also important. Driving into a car park full of battered cars in a shiny BMW or Mercedes is not appropriate, but this scenario could also work in reverse - if the establishment is frequented by wealthy people. Car choice is just part of the preparation, but a very important one.

An external surveillance of the bar will also reveal the dress sense of those entering the establishment; if it is frequented by older people, youngsters, parties, couples etc. This will enable the team to determine what type of person actually visits the bar. The operatives are invited to create a cover story in the event he or she is asked questions in the bar, such as "where do you live?" - "what do you do?" "where do you work" etc. Conversation in a bar is often 'off the cuff' and such questions arise frequently over the course of a drink or snack. Most contact surveillance officers will relate a conventional cover story - utilising real companies that are close by, or noting a street name on a nearby housing estate. Attention to detail is vital prior to embarking on such an operation.

At some stage the bar must be entered, even if an ordinary surveillance reveals the target's home address. (The bar itself could be used as a

Surveillance officers will utilise both sides of the pavement - and occasionally fake a breakdown



Run-down and looking a little menacing - this bar and club still has CCTV.

meeting point for other dealers and cash transactions may occur inside.) Like any bar or club, it will be used by locals or regulars who will notice a total stranger. It's important therefore that any cover story used by the operatives appears totally authentic.

In this exercise the trainees know the dealer and his cohorts - they are all colleagues of course, but this very rarely lessens the tension. Nor do they want to fail at the first hurdle by not gathering as much evidence as other participants in the programme.

Once inside the bar, the operatives are invited to examine the possibility of placing cameras and recorders in concealed areas. It's essential some type of imagery is taken for analysis by the team as a whole. The ceiling of the bar may be by suspended enabling cameras to be positioned in the roof space. A particular type of smoke alarm could be installed. These could be exchanged for identical units carrying covert cameras or



listening devices. Air vents, PIR units, music speakers, picture frames, televisions, ornaments, seats etc. are also useful concealment objects.

However, many establishments now have CCTV, and suspicious activity could be recorded. An experienced surveillance officer will note the type of camera[s] being used and evaluate their potential.

In this test trainees use surveillance devices concealed on their person. There are many available on the market, but carrying a camera or listening device always poses some risk. In two recent BBC undercover documentaries (one on illegal payments in the football transfer market, and the other on the activities of rogue bailiffs), the corporation used equipment that provided excellent images and sound quality. However, one button camera shone red and alerted one of the men being investigated, while staff at the money recovery company actually discovered an adapted video camera in the handbag of a female undercover reporter. Amazingly, the acting ability of both reporters enabled them to escape these tricky situations and continue their role play.

ON-SITE INVESTIGATION

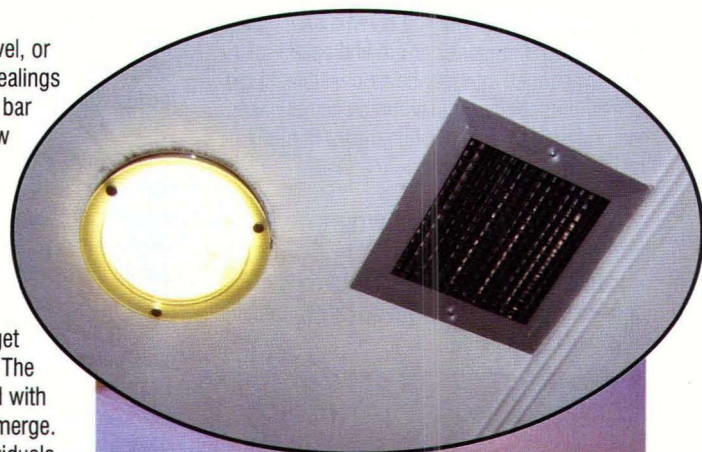
Before selecting any body-worn equipment, the trainees must evaluate the lighting inside the bar. Some cameras work well in changeable light, but others perform dreadfully, thus a little time and analysis should be given to this factor. Initially, the trainee is given advice on the type of system to use and where best to conceal the devices.

Once the target has been identified, the operative has an opportunity to collect video footage or still photographs, note his favourite place in the bar etc. (a small recorder could be placed under the table or chair). More importantly, they must determine if the target is interacting with other

clients on a purely personal level, or whether or not more sinister dealings are afoot. Spending hours in a bar is not an ideal situation, yet few people will notice anything untoward if the time span is 20 or 30 minutes. Intelligence gathering is often played out over a period of time, thus the trainees are taught not to chance their arm by trying to get all the information in one visit. The operatives will also be charged with learning of any patterns that emerge. The target may meet with individuals on specific days or at a certain time. This type of information is helpful in establishing a picture, and in the event that the surveillance may be broadened to encompass the target's colleagues.

Obtaining names can be difficult, but in time, eavesdropping on conversations or the barman's chatter can prove rewarding. Nicknames may be called out by his friends or other places the target visits. Monitoring the use of the target's cell phone and the arrival of colleagues thereafter could expose more leads. If the target uses the local bar telephone, instead of his cellphone - it could suggest he believes his phone is being monitored. Noting counter-surveillance methods gives the surveillance officer warning that the target is concerned about his activities.

When a professional surveillance occurs that involves the placing of listening devices and cameras in a private building, a warrant is always



The air vent in this washroom is ideal to position a covert camera. Note the nearby light. By routing a power line to the camera it would enable continuous surveillance. It also negates the use of batteries



REFLECTIONS AND MIRRORS

Using every available means to track targets and vehicles is taught to trainees at MI5 from an early stage. In these three images note how the operative utilises the reflection from an office building, a restaurant, and finally a vehicle. In all cases there is no eye contact

already observed in the bar. The operative should by now be able to determine if the target is using counter-surveillance methods, but a surveillance analyst is taught not to read too much into unusual behaviour. Closing curtains during the daytime may simply mean he is taking a nap, but it could also indicate he is performing tasks that are decidedly illegal, such as the packing of drugs or even manufacturing them.

Throughout a surveillance of the bar and target's home, the trainees will write down the registration numbers of all visiting or suspicious vehicles. This is an essential security trait that analysts (and ultimately the courts) may use. Cross-referencing such numbers with those identified in the bar's car park, for example, can be useful in determining more patterns.

LOSING CONTACT

Surveillance is often a time-consuming and mundane affair, especially if contact is lost over a period of a few days - and that happens - especially if the target uses counter-measures. Trainees are taught never to drop their guard - even for a few seconds. Loss of contact could mean the target has gone on holiday, is visiting friends, laying low for a while, or has gone further underground. There are a number of

required. But that's as easy as it gets. Installing such equipment in a residence, bar or office requires a thorough surveillance and cunning. Surveillance teams will monitor the movement of those working in or managing the bar: when it is not manned, or a time-slot when devices can be installed. However, the owner could be willing to help the authorities, but asking for his or her cooperation always runs the risk of exposure, and it's possible they too could be involved with the illegal activities.

MI5 are experienced in this field and use highly secret methods to infiltrate locations and install necessary equipment. Few bar owners would question a delivery man or a plumber arriving to

fix a leaking waterpipe. The trainees are invited to create scenarios allowing team members time to install devices - and if that means cutting a wire or moving a few slates from the roof - then so be it!

HOME ALONE

A surveillance on the target's house or apartment will always provide a plethora of useful information. Sifting through garbage can uncover discarded notes, receipts, invoices, telephone bills and scribbled messages. Trainees are taught that sometimes getting your hands dirty can be very rewarding. Equally as important, a photo surveillance will help identify any visitors to the house - some may 'match up' with people



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"



EYE SPY SURVEILLANCE COMPETITION

Test your observation skills

Once inside the bar, the trainee can surveill the location and note any object, fitting etc. that could be useful if surveillance equipment needs to be installed. In this authentic covert photograph there are at least eight locations ideal for placing cameras and audio devices. Send your answers to Eye Spy in the UK. Correct papers will be entered into our prize draw (drawn on 1 December). Three readers identifying the most locations will win Eye Spy's best-selling SPYFINDER - a covert camera detector worth £125.00. A high-resolution image can be downloaded at www.eyespyimag.com under 'Surveillance Competition' (front page). Readers can also send their answers via the website. We've already given you a start - note the PIR sensor that can be exchanged for a covert camera.



WIN A SPYFINDER - COVERT CAMERA DETECTOR



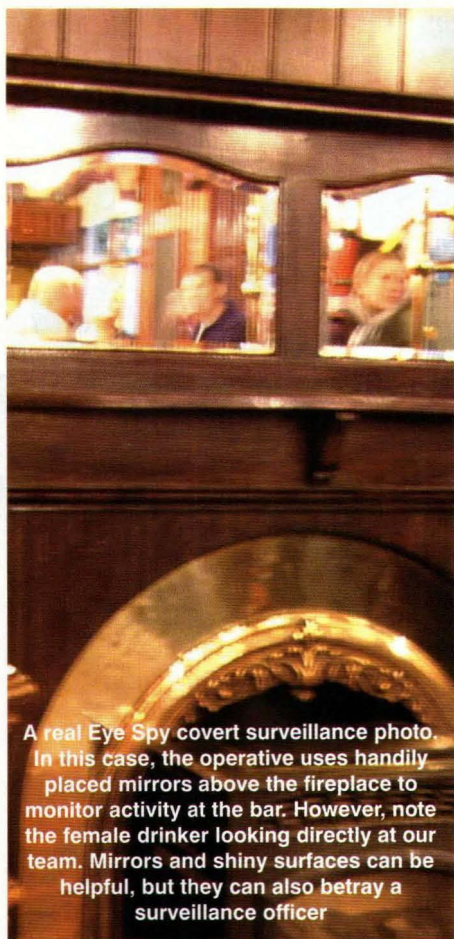
ways the trainees can determine if the target is indoors.

If the target's home telephone number has been discovered, a simple phone call to the premises can be made resulting in a "sorry - I dialled the wrong number". A trace on the target's cell phone will also reveal the general area of his whereabouts - unless it is being used by another person. Monitoring lighting in the house or listening to a television or radio is not always proof enough he is still indoors. Inexpensive equipment can turn electrical equipment on and off in a random manner. Surveillance officers can get near the premises by posing as a postman, for example. A through-wall listening device could reveal movement or conversation. If no-one is at home, entry can be made and a proper search of the apartment is possible - but it's a risky business.

If the target's car is still in place, various options exist that will reveal if the vehicle has been driven. Twenty-four hour surveillance is always enabled, but officers can resort to other methods to confirm if the target is still indoors. A tiny stone placed on the wheel will fall off if the vehicle is moved, or a plastic or paper cup can be positioned so it will be crushed. Similarly, a black thread can be loosely fixed across the front door with spray glue and will be moved if the target exits or enters the house. A mounting number of milk bottles or unopened mail behind the letter box offers further clues. If the target has been seen getting into a taxi or friend's vehicle with suitcases before contact was lost, it's more likely a holiday is the reason for his departure - but it could also mean he has discovered the surveillance and fled. However, a trainee is taught time and time again to "never assume".

Surveillance cameras - even when covertly hidden on the person or fixed in hidden objects and places does not necessarily mean they won't be discovered. A recent undercover BBC operation was nearly blown after the camera (lens) hidden behind a button caught the light and shone red - as seen in this image. The camera in this case is not even transmitting

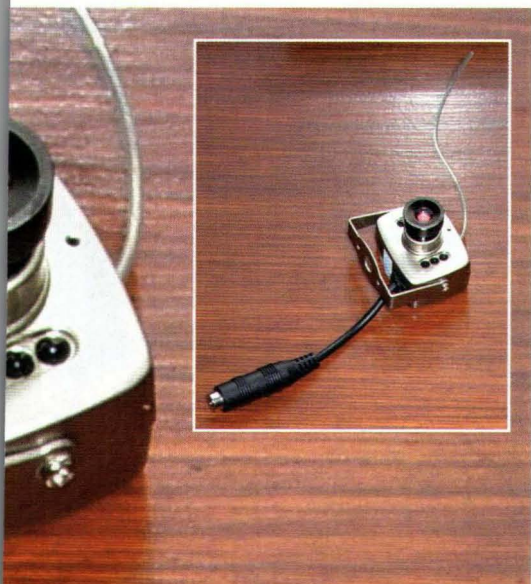




A real Eye Spy covert surveillance photo. In this case, the operative uses handily placed mirrors above the fireplace to monitor activity at the bar. However, note the female drinker looking directly at our team. Mirrors and shiny surfaces can be helpful, but they can also betray a surveillance officer

Surveillance skills can be taught, but the trainee must also have the ability to absorb information and respond accordingly. It's not for the fainthearted, but with the proper training and much enthusiasm, a determined person can succeed, after all, the main role of a street surveillance officer is to simply act normally in everyday situations. The real skill is remaining invisible, having the ability to converse with colleagues, gather intelligence and make calculated decisions.

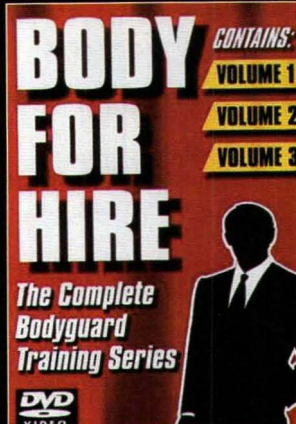
In the exercise depicted here the trainees should have achieved most, if not all of their objectives.



BODY FOR HIRE

THE COMPLETE BODYGUARD TRAINING SERIES FOR STUDENTS AND PROFESSIONALS ALIKE

Three Disk DVD Set - Nearly six hours of lessons and training. Featuring: Rick Reynolds, Bill Thompson
Director: James DePalma



"ESSENTIAL VIEWING FOR THOSE EMBARKING ON A CAREER IN THE SECURITY INDUSTRY"



PLEASE NOTE: These DVDs will only play on machines in the USA Canada and Region 1. UK and European readers should contact Eye Spy Intelligence Magazine for further information

Available from Eye Spy: Ref: BFH/3 UK £90.00 US \$125.00 ROW £95.00
use order form on page 82

PPA INTERNATIONAL & ORION GROUP STRATEGIES

Learn the skills necessary to work in the close protection industry



After years of successes in the European market PPA International and Orion Group Strategies are now offering courses in the United States of America

Visit our website for additional information on courses and announcements:

www.ppa-int.com or www.oriongroupstrategies.com



For a free information pack e-mail: info@ppa-int.com or visit www.ppa-int.com

Tel. +45 47 77 17 36

SURPRISE MAIL

LETTER BOMBS AND RISK AS

Eye Spy looks at what should and should not be done when a suspicious package or letter arrives on your door step.



It's the easiest, though hardly the most effective way to deliver a bomb or deadly substance to a location, office or individual. During its journey a multitude of things can happen to a package that results in it not reaching its destination, yet despite spectacular advances in mail security and screening, the odd item will get through. However, the sender will always be uncertain, and furthermore, once the item is discovered, tests can take place on its content, outer-packaging and from whence it came and was posted. Eye Spy has learned that terrorists are again examining the 'route one' method to deliver their deadly message. Sadly, it's likely those working in the delivery system are more vulnerable than the intended receiver. But there are actions and procedures that can lessen the risk.

Parcel and letter bombs, anthrax-laced envelopes and other devices have caused mayhem in the past. Letter bombs may be explosive or incendiary (the two most likely kinds), or conceivably chemical, biological or radiological. People have lost fingers, eye sight and some have even paid the ultimate price for not recognising a suspicious package. Furthermore, items laced with anthrax have come apart in postal machinery and innocent workers have been killed.

Since the deadly anthrax attacks in Washington DC and elsewhere in the USA that followed 9/11, huge efforts have been put in place to alert workers to the dangers in sorting offices. Devices and 'sniffer' machines are 99% successful in identifying such materials, but there are always going to be instances where dangerous packages get through to their intended location. Similarly, courier firms are now so numerous and not all have the same type of security that organisations like the

Royal Mail or US Postal Service employ. Of additional interest, unless the package is delivered by courier, a letter bomb is unlikely to contain a timing device. So, do you know the warning signs of a potentially dangerous letter or package? And what to do if you come across one? These questions were raised by the security services endeavouring to advise not only postal workers, but employees of firms and individuals who are often the first to open mail - and this also includes ordinary members of the public - mail sometimes gets delivered to the wrong address.

In recent years major government poster campaigns warning of terrorism, cyber terrorism, espionage, and general safety, including what to do in the event of a serious biological incident, have become more and more prominent. Spread across London, New York and other major cities it's not uncommon to see security service posters request the





ESSMENT

*Intelligence
watchers note the
dangers of letter
and parcel bombs*

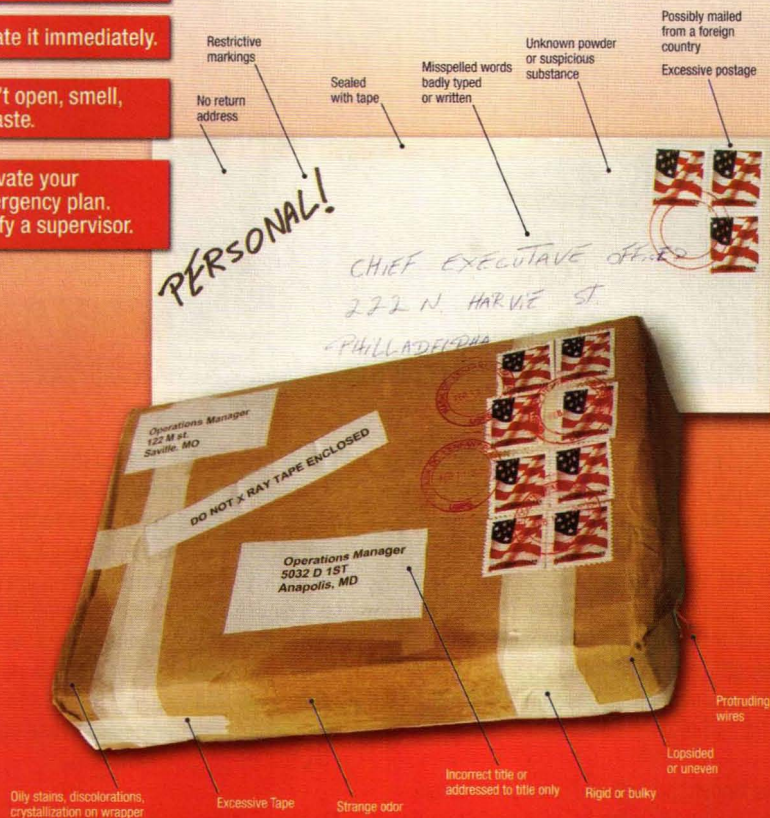
public come forward if they observe anything suspicious. Connected to a recent security campaign in London, Scotland Yard produced a clever arrangement of posters giving clues to what the public should look out for - be it unusual activity at a storage lock-up, or bizarre behaviour from persons. At virtually every major transit point in Europe or North America, the public will come across posters and guidance that warn to be fully alert and report unusual items or activity. The posters are produced for no other reason than to help defend against the growing menace of terrorism and for personal safety. The scale of the threat is such that in September 2006, Sir Ian Blair, Scotland Yard's most senior police officer said: "In all my years in the force, I have

SUSPICIOUS MAIL OR PACKAGES

Protect yourself, your business, and your mailroom

If you receive a suspicious letter or package:

- Stop. Don't handle.
- Isolate it immediately.
- Don't open, smell, or taste.
- Activate your emergency plan. Notify a supervisor.



If you suspect the mail or package contains a bomb (explosive), or radiological, biological, or chemical threat:

- Isolate area immediately
- Call 911
- Wash your hands with soap and water



UNITED STATES POSTAL SERVICE



Poster 84
August 2006
PSN 7880-01-000-7087

Engineering the flow of communication

Verify
Messengers

Engineering the flow of communication

SIGN
for Packages

Engineering the flow of communication

Monitor
Access



Forensic specialists wearing anti-contamination suits check for anthrax during the 2001 scare

never known the threat to be so dangerous... it is extremely grave." A further terrorist attack in the UK is utterly inevitable.

In the past, terrorists, crime lords and simple thugs bypassed security on the street, transit systems and locations, by sending their "message" in a box or envelope. It's now on the security agenda again, especially in the UK and United States.

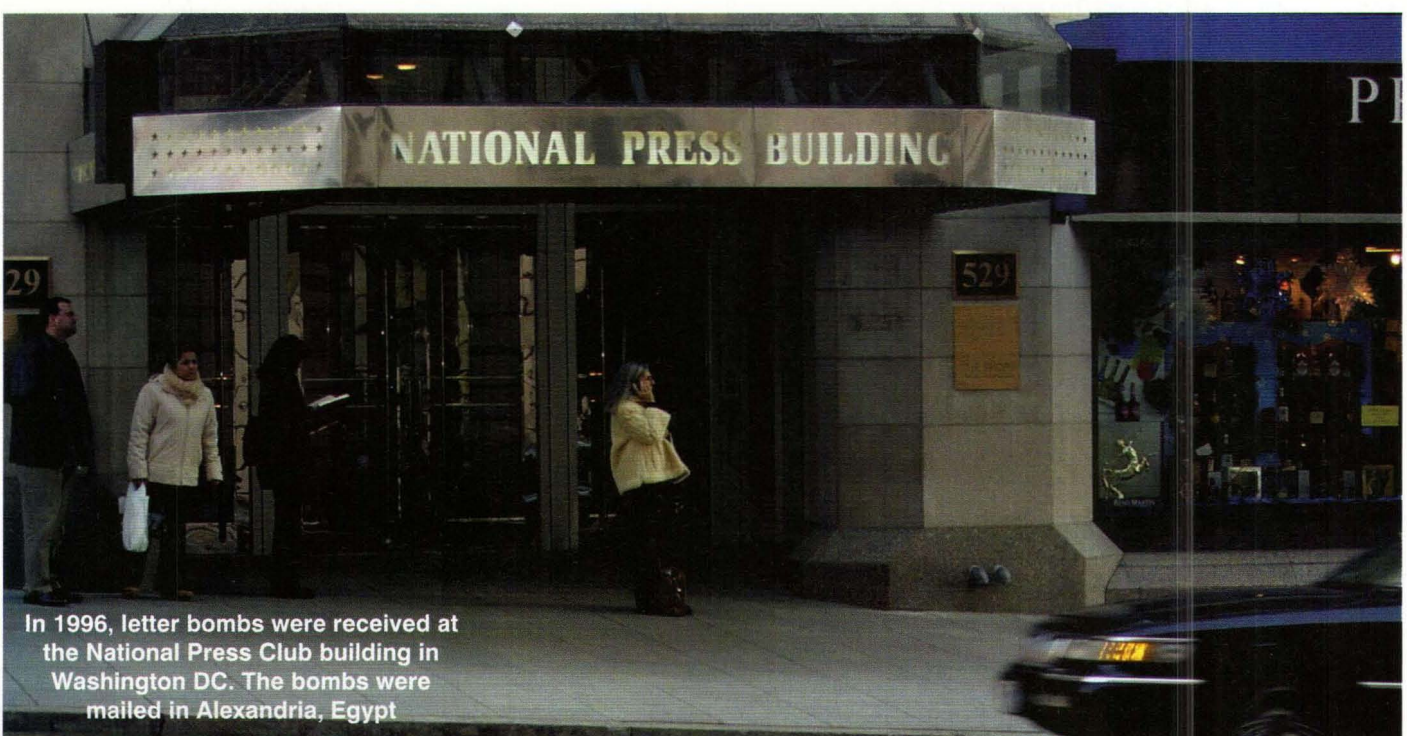
This is evidenced with the release of a new poster produced by intelligence and security experts from four major US intelligence and government agencies: Department of Homeland Security, US Postal Service and its Postal Inspection Service, the Bureau of Alcohol,

Tobacco, Firearms and Explosives and the FBI. Dubbed 'The Suspicious Mail or Packages Poster', it contains vital clues to the possible content of a suspicious package and the necessary steps that must be taken if such an item lands in your office or home. Prior to this poster, all four organisations had their own ideas on what to look for, but this new version is more instructive and concise and brings together the experience of several senior officials.

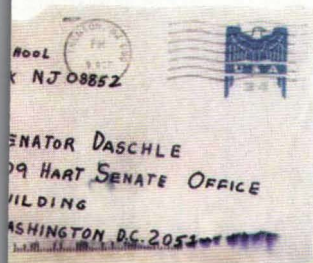
There are thousands of incidents every year across the world. But it's hardly a new phenomena. Deadly packages are usually sent for a reason. Newspapers, politicians, pressure groups, individuals and even the lovers of

cheating spouses have received a nasty surprise in the mail. The following case examples are taken directly from FBI alerts:

01/08/97 - PHILADELPHIA - Federal authorities have charged a 31-year-old Philadelphia man with trying to mail a home-made bomb to President Clinton, [the Philadelphia Inquirer reported Wednesday.] An official of the US Attorney's office declined to discuss the report, other than to say he was familiar with the case. According to the Inquirer, Joseph Washington was charged on Monday with trying to send a padded envelope containing a plastic bottle filled with a flammable liquid and a wick to the White House. It was intercepted last Thursday after postal officials X-rayed it at



In 1996, letter bombs were received at the National Press Club building in Washington DC. The bombs were mailed in Alexandria, Egypt



THE AMERITHRAX INVESTIGATION

Soon after the terrorist attacks of 9/11, letters laced with anthrax began appearing in the US mail. Five Americans were killed - and millions of people terrorised. It was the worst biological attacks in USA history.

The ensuing investigation by the FBI and its partners - code-named "Amerithrax" - was one of the largest and most complex in the history of law enforcement. Today, the FBI remain determined to solve the case. The Bureau conducted more than 9,000 interviews and issued some 6,000 subpoenas. Nearly 20 FBI agents, working with inspectors from the US Postal Service, continue to pursue each and every lead aggressively.

the Fairmount branch post office. The Inquirer said the man voluntarily admitted himself to a psychiatric hospital after he was charged.

01/03/96 - Washington, DC - The FBI has this evening issued a warning about letter bombs, mailed from Alexandria, Egypt, and received at the National Press Club building in Washington DC. Seven devices were received at the offices of the Al-Hayat, an Arabic newspaper. They were described as being in plain, white envelopes, 5 1/2" X 6 1/2", with computer-generated addresses, no return address. They were post-marked on or around Dec. 21, 1996 from an Egyptian post office. They appeared to be Christmas cards.

Greeting cards are getting more sophisticated every year. Those that contain an audible

message are fitted with electronic devices. These products can be adapted with deadly intent. Take this FBI signal, for example:

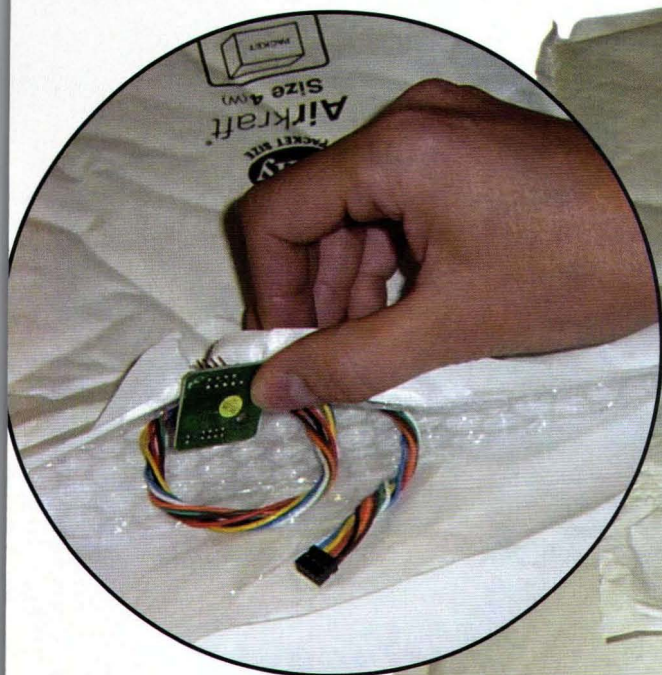
SECURITY ALERT - issued 12/24/97 via ENN Daily Report - Vol. 2, No. 359 - By: Paul Copher, ENN Counter-Terrorist Analyst-at-Large. The nice Christmas cards that use tiny circuit boards to play music when opened are now being bought and can be used to act as the final circuit in the detonation of letter bombs. The device is removed from the card and fixed to the letter bomb. The flat DataSheet, Flex-X or even thinly cut and rolled out C-4 can be fitted with a detonator and the wiring tied into the musical circuit board. The tiny battery in the board has been found to have enough of a charge to fire some detonators. The explosive can then be fitted into a

magazine or book. When opened the circuit will send the detonator a current of electricity and detonate the blasting cap and explosive.

Christmas is always a nightmare for the security services. Hundreds of millions of cards and gifts ply their way through sorting offices across the globe, and of course, everyone loves to receive such items. However, for the more discerning terrorist or criminal, it's not too difficult to find when the intended target's birth date is and send a 'birthday card'.

Continued on page 66

Never open a package with protruding wires. A favourite method used by terrorists is to attach a detonator to the seal of a padded envelope. Once broken, it will detonate any contained explosives



TRADECRAFT

INFILTRATION

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...



Depending on the environment, circumstances, and often country of operation, working undercover and acquiring and communicating intelligence poses major problems.

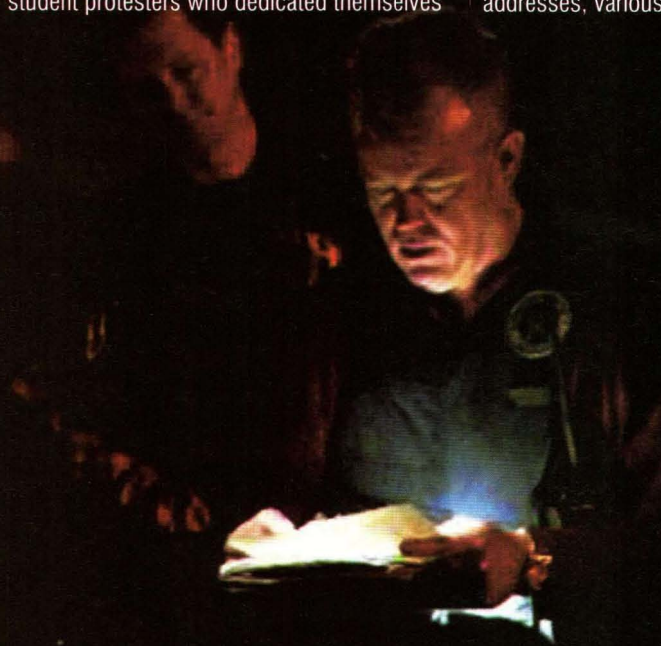
Infiltrating a suspected terrorist cell, crime gang or any illegal operation with an embedded operative is both difficult and dangerous, but not impossible. In recent times at least six suspected terrorist cells in Canada, Britain and America, have been successfully infiltrated by actual operatives. In each case the members of the cells 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.

Al-Qaida has long used the "pyramid technique" whereby if a terrorist is identified and arrested, he will not be able to expose all the members of the group. A terror cell will operate in secrecy, use pseudonyms, false addresses, various identities and communi-

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...



-cate covertly, often in code. The cell will rarely meet as a group, but if this does happen, the location can either be covert or overt. A prime example of an overt meeting occurred recently in London, whereby a dozen or so suspects were arrested as they sat down in a restaurant. Few would suspect a group of people enjoying an evening meal - a scenario that happens all the time.

Since the dismantling of many sleeper cells in the last three years, terrorist operatives or those who support such people have started to use additional security measures. This has made it more difficult for organisations like MI5 to infiltrate, but the service has a long history of success in this area. Experience in countering terrorism was forged in Northern Ireland, and since the end of the conflict, it has been revealed that MI5 had agents deep within the IRA and its hierarchy.

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.



Preparing a cover story prior to any attempt of infiltration is vital. In many cases, terrorist members of a cell will check details, background, paperwork, identity and can even invite the undercover operative to perform certain tasks

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.

Surveillance teams will also monitor everyday purchases and travel. Once vehicles have been identified, this can lead to other members and occasionally, expose buildings where articles or purchases are stored (bomb making equipment, monies, false documentation for example).



An undercover agent is trained to monitor his surroundings and absorb as much intelligence as possible. For example, in this case a casual glance inside an open drawer reveals a set of photos of Times Square, a Lloyds bank book, a membership card to a local martial arts club, a photographer's address, travellers cheques and cash. Obtaining any item could provide fingerprint or DNA evidence (inset)

This is all good detective work and will provide the authorities with excellent intelligence, but what if the group intentions are obscure or the only thing that really exists is suspicion? Similarly, cell members change names frequently, thus confusing those charged with intercepting calls or letters.

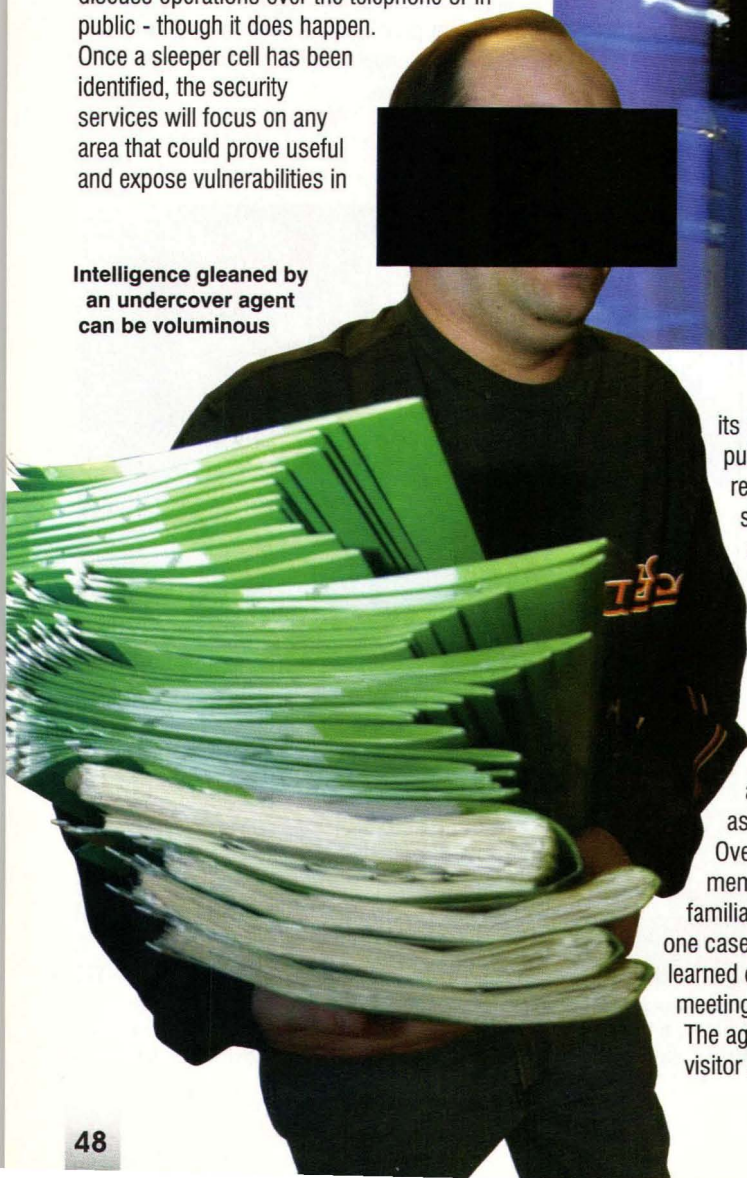
Infiltration is an art, and its highly unlikely core members would except a total stranger joining its ranks without asking questions or performing multiple checks. This is when undercover work starts to get interesting and the minds of intelligence officials and specialists work overtime. Creating layers 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.

To infiltrate any organisation, be accepted and trusted is a number one priority. Just like spies, terrorists or those who support groups such as al-Qaida can and do get over confident. Henceforth, core members, planners and those in charge tend not to discuss operations over the telephone or in public - though it does happen. Once a sleeper cell has been identified, the security services will focus on any area that could prove useful and expose vulnerabilities in

Intelligence gleaned by an undercover agent can be voluminous

GAINING CONFIDENCE

Eye Spy learned of a US-based terror cell meeting regularly in a pool hall. The agent became a frequent visitor and eventually befriended the group.



its operational duties. If a public meeting place - a restaurant, library, club or similar is used by cell members, it's possible to get close to those involved simply by placing an undercover agent in the area.

"Listening" is a valuable asset and an agent may overhear a conversation and make a gesture such as a "nod of agreement". Over a period of time, cell members may become familiar with the agent's face. In one case example, Eye Spy learned of a US-based terror cell meeting regularly in a pool hall. The agent became a frequent visitor and eventually befriended

the group. During the course of several months, he managed to gain their confidence and ultimately their friendship. Meanwhile, two companies had been established - a travel bureau and an army surplus store - both fronted by security officers. The undercover agent said they were "secure" and invited cell members to visit the shops. The "managers" confirmed his "reality" as a neighbour and also befriended the cell members. The illusion worked: the shops and staff provided assurance and insurance - a vital tool in respect of concealing the agent's real identity. Purchases were then made and requests given to the agent revealed the group's intent. The plan worked and a sting operation followed.

Double Jeopardy

It can be helpful if the security services obtain the help of persons who are friendly with suspected cell members - a neighbour for



An operative who successfully infiltrates a terrorist cell or group will provide intelligence on the locations used or frequented by the suspects. This is used by the security services in future raids or searches. Knowing which room is used to store materials or used for meetings is invaluable

example. However, it can be problematic - the person may notify cell members that they are being monitored, or even provide disinformation. An undercover operation may also be exposed before all the evidence has been acquired, thus, it's an avenue that some intelligence officials deem too risky.

Eyes and Ears

MI5 are particularly good at infiltration - getting agents close to surveilled targets. Its methods are highly secret, but depending on the type of operation, agents will be outfitted,

groomed and fully informed of the task in hand. Infiltrating al-Qaida in the UK, may or may not involve MI5's highly regarded Muslim officers and agents.

Working alongside persons planning a terrorist operation or performing tasks that support terrorism is advantageous.

An agent may be able to:

Intelligence can be gleaned from suspicious packages as this from the security tape, address label, delivery company and even the barcode



In certain circumstances an agent may have an opportunity to install a surveillance device - or at least identify a prime location for colleagues to perform such a task

1. Detect real names.
2. Obtain paperwork.
3. Obtain forensics (i.e.. fingerprints, DNA).
4. Identify new faces.
5. Place listening devices.
6. Note how funds are transferred, collected and what currency (cash) is being used.
7. Discover who is assigned the task of purchasing equipment, hiring vehicles or similar.
8. Identify the senior cell members.
9. Ask disguised questions.
10. Learn of connections to other local groups.

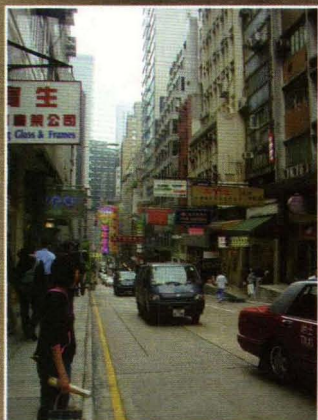


Many of the points on the previous list are factors that ordinary electronic or foot/mobile surveillance may not be able to detect, especially if the group uses advanced counter-surveillance methods.

If invited to houses, meeting rooms or other locations, the agent then has the opportunity to note his surroundings and other details, including any unusual items. Memorising the delivery address of a suspicious packet or even the carrier may prove useful. Any intelligence that can be gleaned from such items affords the police or security services with an opportunity to augment the operation. For example, if the group regularly uses one postal delivery company, it's likely it too can be surveilled and the contents of the packages researched more fully. Similarly, it won't take long to discover where the item was despatched from. Even noting a few numbers from a barcode can be rewarding.

The Ladder

If the sleeper cell has international connections, it is often possible to infiltrate associated groups or individuals in foreign countries. One this has been achieved, "recommendations" can be made - the purchasing of equipment or explosives etc. Of course the recommended person or company will be bogus and fronted by agents. A cell member thousands of miles away unaware of the ruse will trust the person and an association will form - after all, his name was given by a trusted colleague. In time, the cell will be breached and valuable intelligence gleaned. It's a method that has been used to expose spies for decades and is now being adapted to help "out" existing threats in dozens of countries. A hefty cash advance in a foreign country for making a simple phone call "recommending" an undercover agent or front company works almost every time. The intelligence service will look for a weak link, blackmail or similar may follow, including the threat of a prison term. It's underhand, shadowy but legitimate in the world of counter-terrorism and the technique helps get the security service climbing the ladder until it is inside the terror cell.



It's both awkward and dangerous if the undercover agent is asked by group members to participate in the actual operation. Delivering a package to a 'colleague' or collecting travel documents means the operative must be tracked for his own safety throughout his journey by fellow security officers. His journey could even take him out of the country. Terrorists now employ counter-measures that could expose suspicious behaviour



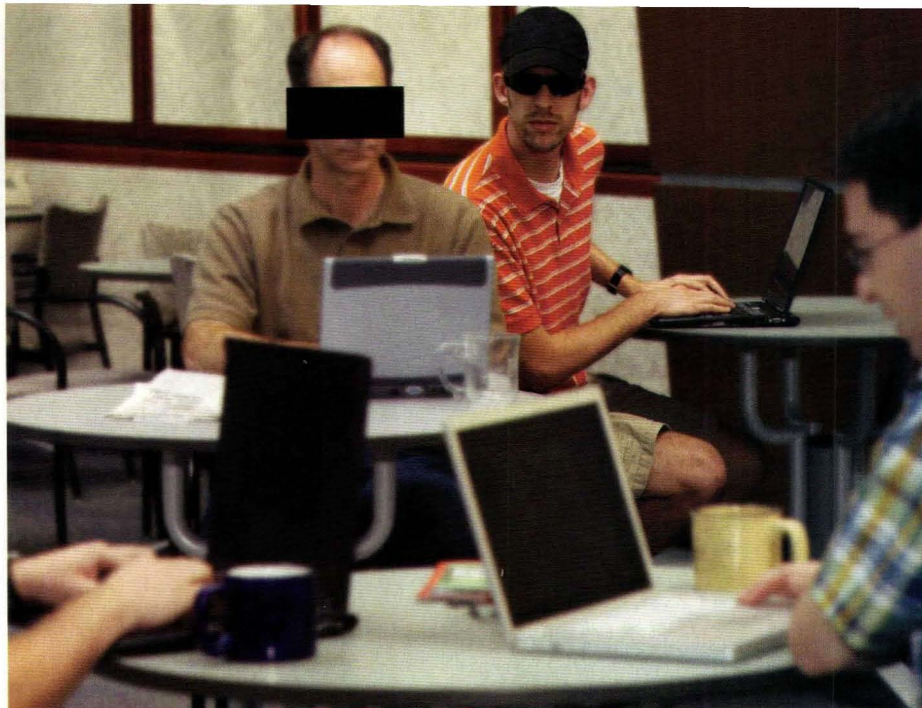
Once away from the terror cell, agents will be debriefed by senior officers. The agent can also relate information in more detail

Searching for a weak link is a specialist task. "Turning" an actual cell member risks revealing an investigation is underway. However, the suspect may feel that he has nothing to lose because the plot has been exposed anyway - and it may save him from a lengthy prison term. Infiltrating a sleeper cell using this technique has been questioned by senior analysts, including Nick Pratt of the George C. Marshall European Center for Security Studies based in Germany. He warned: "Al-Qaida is held together by bonds of friendship, kinship and discipleship."

MI5 has specialist agents well-groomed in the art of infiltration, but occasionally, operatives must perform tasks alongside terrorists to help enhance the illusion. This is a controversial area - just ask Kevin Fulton, a British Army agent who operated in the IRA. He built bombs, travelled to New York to purchase bomb-making components, lied and deceived, but all in an effort to help keep his true role invisible.

Infiltration has a unique friend in the Internet. Eye Spy is often asked why the authorities don't shut down al-Qaida's numerous "support" web sites. The answer is simple - visitors to such sites can be identified. Similarly, they offer an incredible amount of intelligence, be it a concealed message from a terror leader or revealing a planned or conducted operation. By monitoring such sites, organisations like GCHQ or the NSA can analyse traffic and help focus on extended chat rooms. By cross-referencing users, the intelligence world can literally "see" who is a prolific user and examine remarks and comments in detail. It's true certain characters will not use their real names or connect via computers in Internet cafes instead of their own machine or cell phone, but that terminal then becomes an intelligence target - revealing its location, users etc. In the recent USA airliner plot, dozens of Internet Cafe terminals were removed by MI5 and the police because they had been used by the suspects. A correlation with surveillance footage will ensue and the user identified.

If a chat room used by potential terrorists is identified, it's not at all difficult to join in the



Analysis of any intelligence collected by the agent will help authorities plan the next stage of their operation. Similarly, senior analysts must determine if the agent's role is under suspicion - lest his covert role be compromised

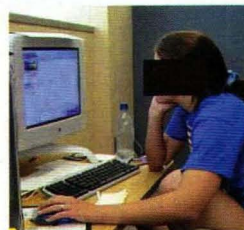
conversation. Once this has been achieved, and the agent has secured his "place on the table" it becomes impossible to question his real identity. "Off the cuff" remarks may lead to an event or a social gathering... once in attendance, the agent has removed himself from the virtual reality of the Internet to the real world. More importantly, his new associates will already be aware of his opinions and background - all perfected by intelligence analysts sitting in Thames House or the FBI's headquarters. It's a time-consuming business, of course, but a valuable method of infiltration. Identifying other chat room users is virtually impossible - as the illustration (above right) shows. In this case a youngster believes she is talking to a young student.

Acting

Getting inside a terror cell is the first step, once that has been achieved, the agent must then function accordingly - even if that means being sent abroad for "training" or performing tasks within the group. However, this does offer additional opportunities for the security services in that they can acquire vital intelligence. If such a venture is deemed too dangerous, an excuse will already have been created.

Passing communications to an "intelligence handler" presents its own problems. Infiltration involves a high degree of planning and prior to any undercover operation codewords, actions, or written words are 'manufactured' to relate or portray previously determined situations. An agent must have the

CHAT ROOMS



Hi. You sound real cute!!
How old are you and what
do you like doing after school?

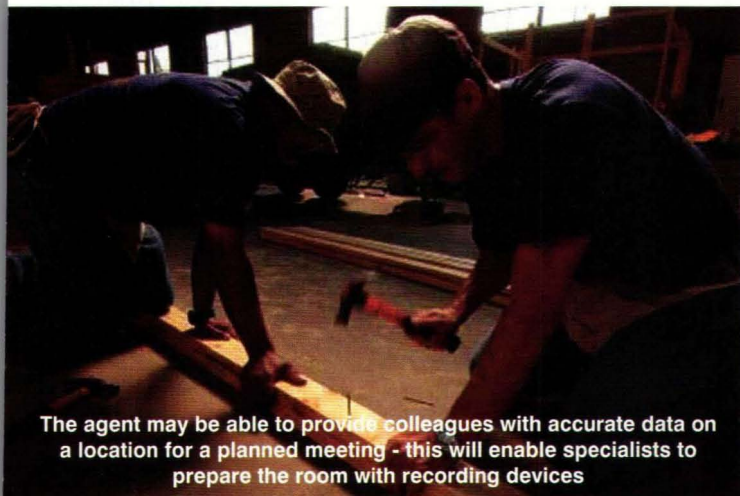


I am 14 and a bit of a fitness
fanatic, I often go power lifting
after school.

ability to make contact immediately with colleagues. Generally such contact is conventional, via personal meetings, telephone or letter. In all cases it must be discreet. An agent will probably be surveilled by colleagues who in turn will be watching to see if his "new friends" are conducting their own surveillance on him.

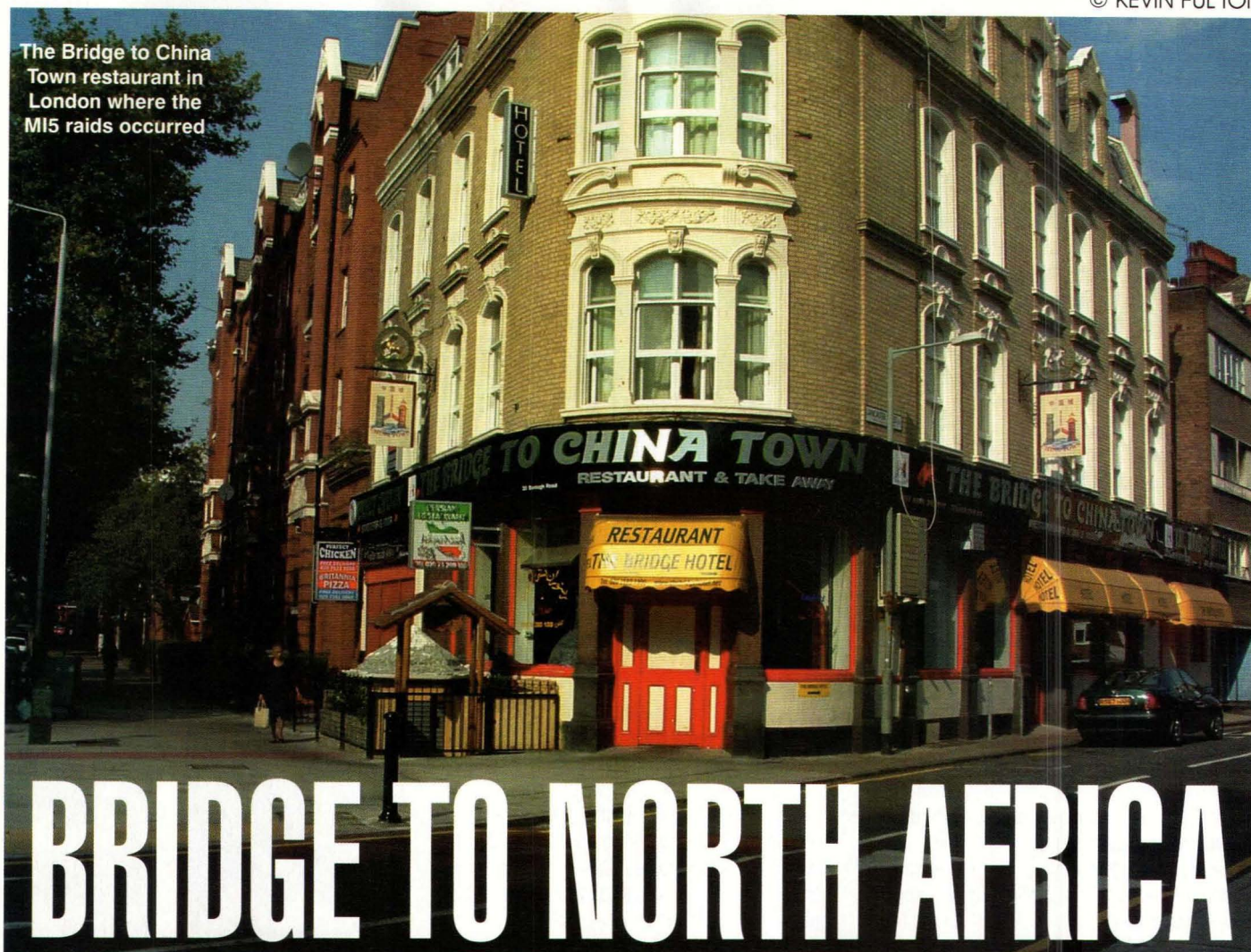
Agents of infiltration are often very good actors. Body language, dress and a manufactured background must be absolutely perfect to carry out such an operation. One wrong response to a question or an odd comment could generate suspicion. A personal cell phone can be helpful and allow the user to call for help, but they can also be dangerous. One call from or to a colleague may alert the group, thus it's important any item carried is "sanitised". Agents must be confident, but not over confident. Their role is to listen, learn and report. All three will ultimately combine to disrupt a plot.

Dozens of al-Qaida franchises have started to appear across the world and the security services are now facing an enemy from within. However, because those involved are predominantly "home grown" and operating from known locations it does offer much more scope to infiltrate suspected sleeper cells. The art of infiltration is a vital area of intelligence and one being taught to new recruits with an added sense of urgency.



The agent may be able to provide colleagues with accurate data on a location for a planned meeting - this will enable specialists to prepare the room with recording devices

The Bridge to China Town restaurant in London where the MI5 raids occurred



BRIDGE TO NORTH AFRICA

Suspected al-Qaida recruiters arrested in London following major surveillance operations across Europe

Following a series of high-profile MI5 operations in the UK, British anti-terrorist police swooped on a restaurant in south London known as The Bridge to China Town and other residential addresses nearby. Officers detained several men who had just started to enjoy an evening meal. The raid was intelligence-led indicating MI5 had monitored the group's movement and were aware of their destination in Borough Road. About 50 armed officers raced into the restaurant at about 10.00pm on 1 September 2006.

The operation, according to high-placed intelligence sources, is in connection with an undercover al-Qaida recruitment outfit that is trying to enrol young British Muslims. It is believed surveillance of several men had led the security services to believe that an attack to "supersede" Britain's "7/7" had been discussed. Targets allegedly included the

London Eye, Buckingham Palace, Canary Wharf and Big Ben. London-based journalists told Eye Spy that two prominent football stadiums were also mentioned. It's not yet known if the group had any ties with other suspected terror cells already under detention in the UK.

Four of the arrested men had reportedly been under surveillance by MI5 and followed via Spain to suspected terrorist training camps in North Africa earlier this year. Three of the names were already held on a police file noting that "discreet vigilance" should be taken. Details of the North African connection came via Madrid. A statement from the office of Alfredo Perez Rubalcaba - Spanish Interior Ministry said:

"In April 2006 as part of a National Police operation into jihadist training camps, police detected and controlled the movement of four of those arrested in London on 1 September.



Alfredo Perez Rubalcaba - Spanish Interior Minister

At the beginning of April the suspects crossed through a land border in the north of Spain and left two days later in a commercial ferry towards north Africa.

"A short time later they returned to Spain by the same route and left Spain in the direction of France by a land frontier. They only used Spanish territory as a passageway. Interested foreign intelligence services were notified."

At the same time, the remote fee-paying Jameah Islameah Islamic school in Sussex, which has just 12 pupils, was also raided. Police searched the £3million former convent and its 54 acres for several weeks. It is believed some of the men arrested in the restaurant were frequent visitors to the school



and allegedly used the grounds to train. A Home Office source said: "The training was extreme and macho. It involved endurance in bad weather and bonding. In that sense it was like combat training."

Analysts have warned senior politicians that the UK is a base for training and "exporting" al-Qaida operatives. MI5 are known to be monitoring the movements and actions of hundreds of suspects who have entered London from conflict areas such as Afghanistan and Chechnya. Al-Qaida manuals and communications discovered in the UK advise sleeper cells should have no more than 14 operatives. Similarly, the manual suggests what type of training can be conducted without attracting any attention.

Several of the men (aged between 17-48) arrested in London have since been charged with terrorist offenses.

- Over ten years ago French intelligence warned their counterparts in London that the capital was being used by al-Qaida. Their fears were dismissed by Downing Street, despite MI5 and MI6 supporting the report.

MI5 - SPANISH INTEL RELATIONS

Cooperation between Spanish intelligence and MI5 and MI6 is at an all time high following transit bombs in London and Madrid. However, the services have a long history of accord. One of the most recent joint operations occurred in 2001 when police raided the homes of two ETA terrorists planning to place 40kg of dynamite aboard the *Val de Loire* ferry travelling from Santander in north Spain to Plymouth, England. Had the bombs been detonated, hundreds of passengers could have been killed.



Val de Loire



Law Enforcement Picture Library

The specialist photo library for law enforcement and related images

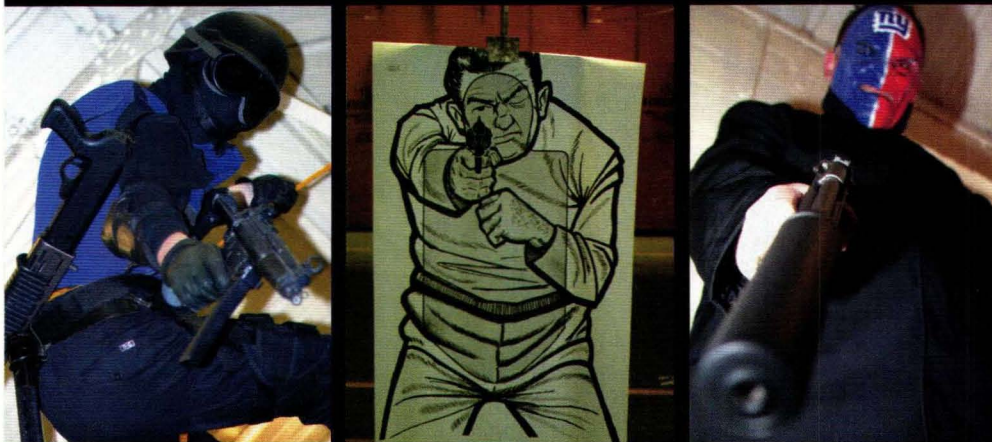
Stock images for all your editorial requirements



Commissions undertaken for location and studio work domestic and foreign



Specialist models and props for advertising, promotional and illustrative requirements



Other services include expert commentary and reporting for media outlets covering legal, law enforcement, terrorism, counterterrorism and intelligence subjects. Law enforcement consultants for Film and Television

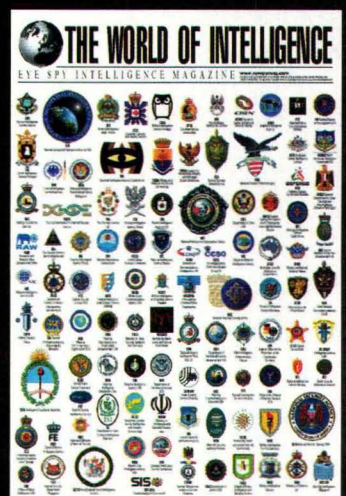


The Law Enforcement Picture Library,
P O Box 33699, London, N16 6YT, UK
Tel: 020 8806 3037 Cell: 07951 054 092

Website: www.lepl.co.uk email: leplinfo@aol.com

SUBSCRIBE TO EYE SPY

CALL NOW AND GET THIS SUPERB
GIANT INTELLIGENCE CRESTS
POSTER FREE



PAY AS YOU GO ESPIONAGE

CIA and other US intelligence agencies look to 'contract agencies' or retired spies to plug 'intel gaps'

It's not unusual for any intelligence agency to use secure "contract firms" for certain tasks, but there is growing concern among some senior officials at the CIA, that the increasing use of 'green badgers' (non-agency personnel who attend secret meetings or perform alongside full time government operatives), may be harmful in the long term. Others disagree, noting the use of contract personnel - many with 20+ years of experience in the field - helps augment current operations and allows new employees time to develop and be trained. "Why throw away years of training and not use it to good measure?" a former intelligence officer told Eye Spy. Nevertheless, intelligence watchers believe if the CIA suddenly stopped using contractors, a serious shortfall in its ability to perform worldwide would result.

In 2004, the US created the National Counterterrorism Center, headed by John Negroponte. More than half those working at the NCC as analysts and advisers are contractors. Similarly, the green badgers - who wear special

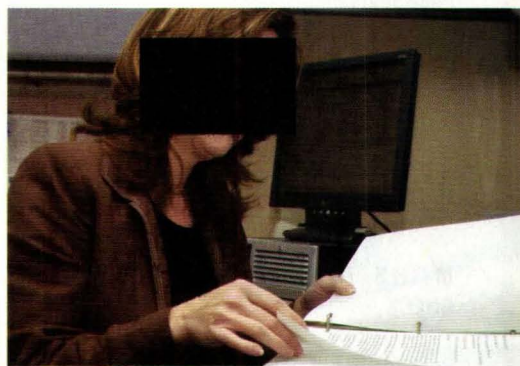
identity cards, are regular visitors to Langley. One well known contract firm in Virginia is made up entirely of retired CIA officers. It's known this company is used to create false identities, cover stories and front companies for many of the CIA's elite overseas operatives. It's a powerful entity that has performed 'tradecraft' for years.

Yet monitoring, liaising, managing and checking the credibility and security of thousands of information providers and gatherers has proven difficult. So much so that earlier this year Negroponte ordered a "comprehensive study" of the use of contractors. America's sixteen premier intelligence organisations from the NSA to the DIA were asked to submit reports on the scale of 'contractor employment' in an endeavour to see if it is "appropriate." The man charged with examining the role of contractors is Ronald Sanders, chief human capital officer for the Director for National Intelligence. In July 2006, Sanders visited Baghdad and spent time with the intelligence community operating in Iraq. He said: "Most are not in uniform; they're civilian employees from all across the intelligence community who have voluntarily placed themselves in harm's way to gather intelligence on our enemies. These are civil servants who are really on the front lines of the global war on terror - indeed, many are in front of the front lines. They are also invisible."

It's almost certain that the CIA's 500-strong presence in Baghdad is outnumbered by non-government intel contractors.

Since the USA was attacked five years ago, hundreds of intelligence-minded civilian agencies have been born - most willing to assist the 'official intelligence community'. Due to the massive investment in security and on-going operations overseas, agencies like the CIA are having to rely more heavily on contract firms doing work once the preserve of its own analysts, foot soldiers and spies. This is despite what DCIA Michael Hayden said in September 2006, noting the CIA's "greatest recruiting drive ever."

Postings may take contractors anywhere in the world



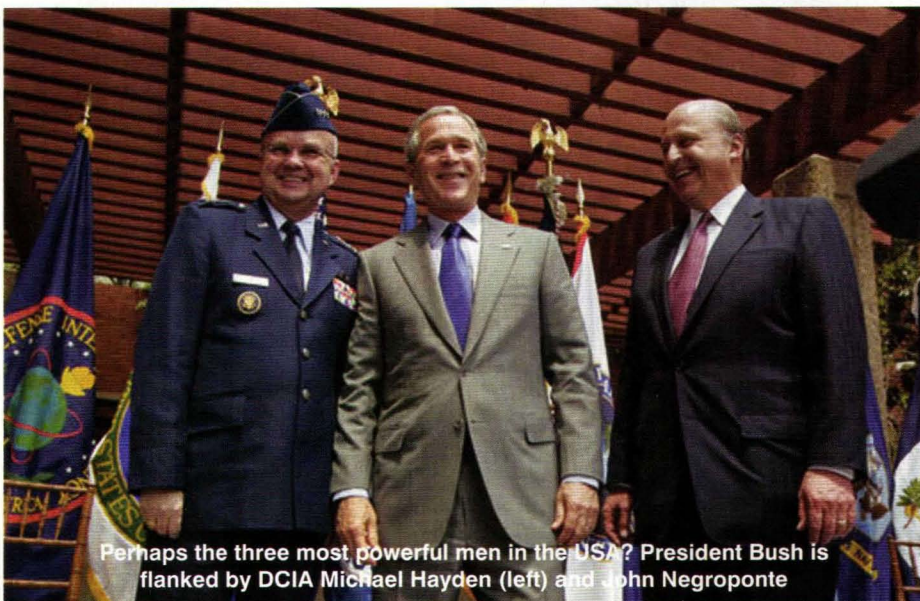
It's not just retired CIA male officers or contractors that are being hired

Interestingly, many former employees are "plugging the gaps" but on a much higher wage - so much so that there is concern within some agencies of a 'brain drain' to the private sector and then a speedy 'return' for higher wages. "We have to come to some conclusion about what our core intelligence mission is and how many [full-time employees] it's going to take to accomplish that mission," Sanders said. "I wish I could tell you it's by design," he said. "But I think it's been by default."

Contracting spies has also drawn criticism from those who believe espionage and intelligence can be likened to a shopping basket - with feats being performed using a price scale. "There's a commercial side to it that I frankly don't like," said James Pavitt, former head of the CIA's clandestine service. "I would much prefer to see staff case officers who are in the chain of command, and making a day-in and day-out conscious decision as civil servants in the intelligence business."

CIA spokesman Paul Gimigliano rejected calls that "out-sourcing" espionage and intelligence

"Contractors give the agency enormous flexibility and are an important part of our work force... as partners, they help us build or enhance specific capabilities we need for a finite period." - Central Intelligence Agency



Perhaps the three most powerful men in the USA? President Bush is flanked by DCIA Michael Hayden (left) and John Negroponte

WORKING FOR THE CIA

The 'Company's' five official 'mythbusters'...

MYTH 1 - YOU'LL NEVER SEE YOUR FAMILY AND FRIENDS AGAIN

The work we do may be secret, but that doesn't mean your life will be. Because the variety of CIA careers is similar to that of any major corporation. So... your friends and family will still be part of your life.

MYTH 2 - EVERYONE DRIVES A SPORTS CAR WITH MACHINE GUNS IN THE TAILPIPES

Car chases through the alleyways of a foreign city are common on TV, but they're not what a CIA career is about. And, they don't compare with the reality of being part of worldwide intelligence operations supporting a global mission.

MYTH 3 - YOU HAVE TO BE SUPERHUMAN IN EVERY WAY

You don't have to know karate or look good in a tuxedo to work at the CIA. But you must possess a deep intellect, the ability to make good decisions and a dedication to serving America through the collection of intelligence.

MYTH 4 - A GLAMOROUS LIFESTYLE AWAITS YOU

Working at the CIA doesn't mean you'll be jet-setting around the globe, attending parties with billionaires and showing off your Tango skills. In reality, we depend on administrative managers and staff for our operational success, at home and abroad.

MYTH 5 - HARDLY ANYONE EVER MAKES IT THROUGH THE BACKGROUND CHECK

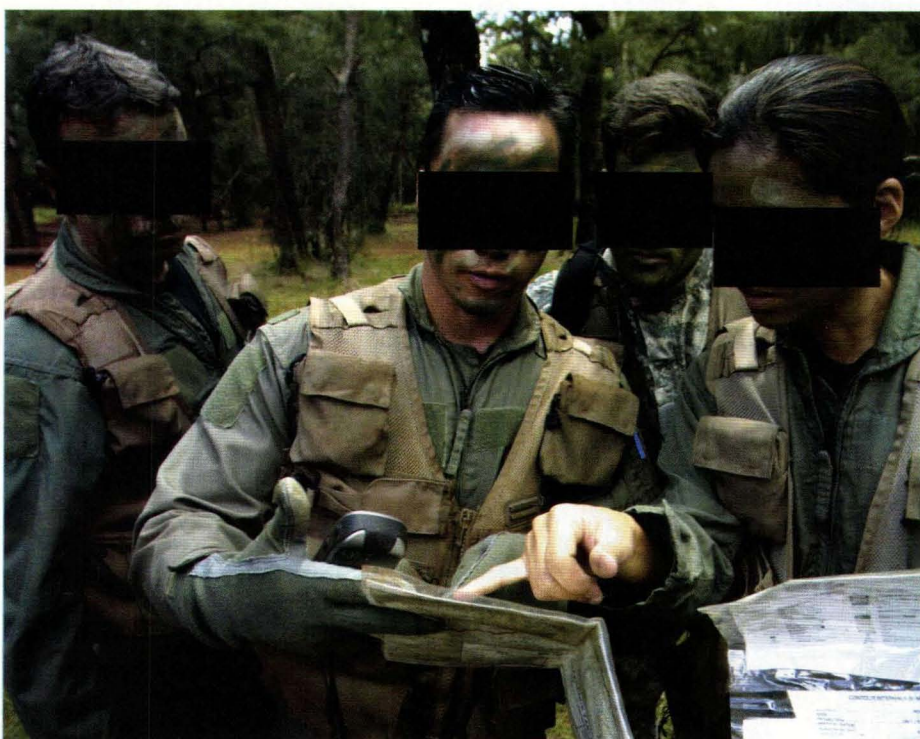
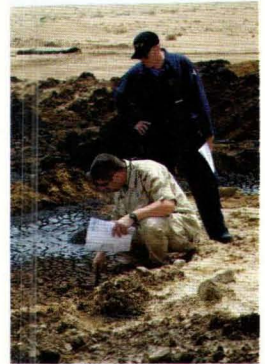
Because of our national security role, CIA applicants must meet specific qualifications - but, don't worry. Getting caught smoking in high school isn't enough to disqualify you. Your intellect, skills, experience and desire to serve the nation are most important to us.

analysis is problematic. "Contractors give the agency enormous flexibility and are an important part of our work force... as partners, they help us build or enhance specific capabilities we need for a finite period." His comments probably reflect the majority in the intelligence community. Many of the CIA's new intel contractors are drawn from the armed services (both serving and retired). And it's interesting to read this comment on the CIA's website recruitment page:

Military service is a good introduction to the important role of intelligence in national decision-making. Many of the CIA's positions require security clearances, specific training and unique life experiences - the same kinds of professional development found in the military. Your patriotism, personal integrity and service to the country don't have to end when your active status does. You can find new direction at the CIA. Explore the vital role the CIA plays in sharing intelligence with branches of the military through the Office of Military Affairs. Consider a career at the CIA and continue to assist your branch of the military.

It's also true that to fully train a CIA case officer takes years. The CIA is probably busier now than at any other time in its history. By paying high wages to retired officers to help the agency in numerous areas, the CIA believes it is generating vital time for new employees to be trained and gather experience. However, the fear is, once trained employees might see greater rewards by leaving the service and then 're-entering' via a secure contract company.

Contractors can find themselves being used on 'active duties', be it gathering informants in faraway lands, or acting as liaison between the CIA and military services. Retired officers - whose background is beyond reproach are again being officially listed and their experience used in specific fields. Yet this is not really the primary concern of those who believe only government employees should handle classified material or attend front-line meetings where top secret operations are discussed. What happens if a breach of security occurs, or an operation involving a contract firm or agent goes wrong? And, just like any agency role, some employees are uneasy about working alongside a contractor on the same operation who will be paid far more for his time. Nevertheless, the CIA is one agency which values the use of contract firms - as long as they are staffed by former employees of 'The Company', or have been recommended by its 'own' or the military. It's an interesting concept.



WINTER COMETH:

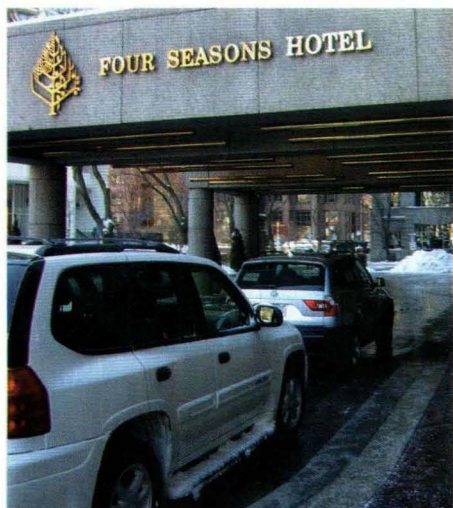
VEHICLE SURVEILLANCE TIPS

During any vehicle surveillance in winter operatives may have to deal with adverse weather conditions. Eye Spy's surveillance advisors have listed a few points of interest - some are obvious, some are not so obvious, but all should be mandatory.

Maintaining your vehicle throughout the year should help when winter descends. A full inspection and service is crucial - especially in cold climate areas.

On a lengthy surveillance interior car windows can (and do) begin to fog. The only way to demist glass is to turn the heater on - an action that sometimes means the engine and lights need to be engaged - alerting all around to your position. A small hand-held fan-heater can eradicate most fogging - simply plug into the lighter socket. Similarly, if this fails - make sure you carry a raw potato... a strange item perhaps, but by slicing the vegetable in two and rubbing the fleshy part on the glass, it will help keep away mist and stop the inside from frosting. A chemical inside the potato is responsible. Similarly, there are trade products on the market which have the same affect. Turning on air-conditioning is noisy and may expose your position - especially in a quiet neighbourhood. If all else fails - open the window - but remember to turn off radios.

Exterior windows can be kept free of frost by a de-icer spray, but it's always useful to carry



Checking vehicles - and the weather forecast before any surveillance should be mandatory



windscreen wash and an ice-scraper. In severe weather - anti-freeze can be used - thus a small bottle tucked away in the car can be handy (don't forget an old clean rag to apply the fluid - if you don't want to damage the car's body-work).

Any surveillance, but especially at night can be problematic. For safety, lock the doors and keep the key in the ignition just in case a hurried exit is required.

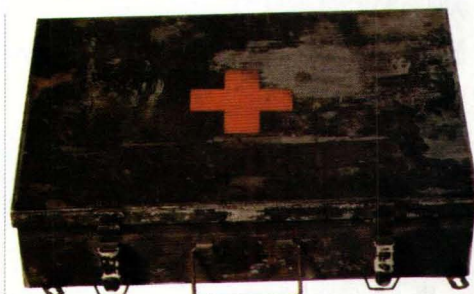
A first aid kit, cell phone and additional batteries to power all equipment are mandatory.

Always carry additional blankets, gloves, boots, warm clothing and lots of hot drinks and food. A thick coat with a hood is also recommended. There are also a wide range of thermal under garments available to warm the entire body. Similarly, there are electric car blankets that can keep an operative warm in the vehicle. All clothing and garments should be dark in colour.

A large bag of salt (grit) can augment your departure in the event that ice has built-up under



Don't get caught out this Winter



A first aid kit is essential

the stationary vehicle - and the car won't move. Don't forget the shovel. Experienced operatives will also carry a fully-charged second battery as night-time and winter surveillance can drain the battery more rapidly than in the summer months.

Placing additional mirrors in the vehicle can be helpful - for both surveillance and security - lest the target or anyone approaches from a point where visual is impossible.

Prior to any winter surveillance, check the weather forecast.

There may be occasions when it is necessary to switch on the internal car lighting. Some lights are extraordinarily bright. Torches that can use variable light are recommended. It's also not a bad idea to carry the odd candle - just in case.

Video and camcorder equipment should be kept dry and the lenses frequently monitored for misting. However, if the operative starts to suffer the effects of hypothermia, using instruments (focusing etc.) is far more difficult. Another reason for keeping warm.

When nature calls it can be problematic. Leaving the vehicle can expose the operative - literally! There is a product available from 'Sportys Catalog', a catalogue for aeroplane pilots and enthusiasts. The container will accommodate both males and females. But if you do have to exit the vehicle - make sure the headlights are switched off. Walking in front of them will make you visible.

2000 VIDEO

Pre-9/11 Video

A video tape dated January 2000 shown on Arab satellite channel Al Jazeera featured Osama bin-Laden meeting with some of the terrorists who participated in the 9/11 attacks on America. It's the third such tape containing movie footage depicting the leader of al-Qaida and the hijackers. Other tapes were released in 2002 and 2003 - both just days prior to 11 September. The film was reportedly made in an Afghanistan training camp.



MI5 Watchers Target Universities

As reported two years ago in Eye Spy, British intelligence is surveilling UK universities in an attempt to expose infiltration by al-Qaida. An 18-page draft report was obtained by a newspaper that outlines plans to monitor the activities of certain sections of the student population. The document, allegedly drafted by the Department for Education acknowledges that some universities may see the move as akin to 'big brother' or that lecturers may feel they are spying for a 'secret police state'.

Eye Spy learned that a number of groups and individuals in some of Britain's leading universities are already under surveillance due to intelligence gleaned from various sources.

The move inviting lecturers to raise their concerns over students with the relevant authorities has already been attacked. Leading academics believe the move "envelopes" all Muslims and Asians. However, the draft report is only a consultation document and is now being examined and discussed at every level.

MI5 and Special Branch are also concerned that a number of

groups are recruiting on campus. The 'recruiters' target young impressionable and sometimes lonely students who may be tempted away from mainstream activities. In future years, these students may be contacted or used for illegal activities. Govern-

ment advisors are hopeful that universities will engage and provide information.

Part of the draft report says: "While radicalisation may not be widespread, there is some evidence to suggest that students

at further and higher educational establishments have been involved in terrorist related activity, which could include actively radicalising fellow students on campus. Perhaps most importantly, universities and colleges provide a fertile recruiting ground for students.

"There are different categories of students who may be 'sucked in' to an Islamist extremist ideology. There are those who may be new to a university or college environment and vulnerable to 'grooming' by individuals with their own agenda as they search for friends and social groups; there are those who may be actively looking for extremist individuals with whom to associate.

"Campuses provide an opportunity for individuals who are already radicalised to form new networks, and extend existing ones."

MI5 has been engaged in an operation to identify al-Qaida recruiters operating in universities. Trying to enable a just and fair plan to monitor and stop the creative influence of such characters is proving both difficult and controversial.



"AN INTEL GEM"

ws Bin-Laden with Hijackers

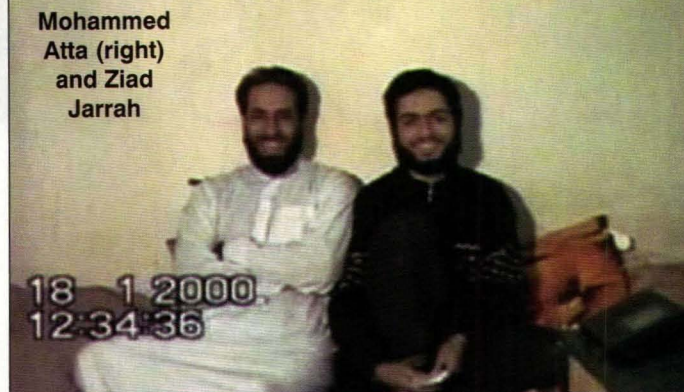
Ramzi Binalshibh, al-Qaida's former paymaster who helped funnel monies into the United States, is shown speaking on the tape, which was aired just days ahead of the fifth anniversary of the hijackings. Bin-Laden is sitting alongside his former lieutenant Mohammed Atef, another suspected planner of the attacks. Atef, also known as Abu Hafs al-Masri, was killed by a US airstrike in Afghanistan in 2001. Binalshibh was captured four years ago in Pakistan and is now in US custody.

Another section shows Mohammed Atta and Ziad Jarrah - two of the 9/

11 hijackers. Both men read their will on camera.

The tape also features hooded men performing martial arts in a courtyard, wrestling over a handgun, and others walking over rugged terrain. Wael al-Shahri and Hamza al-Ghamdi, two of the 19 hijackers are also on the tape.

The video tape, a composite of various scenes, shows Bin-Laden in the middle of a group of armed men - reportedly members of al-Qaida - though their faces are not clear enough for identification. However, some analysts believe other 9/11



hijackers are in this group. Throughout the scenes, Bin-Laden does not speak to the camera. A narration praises the fighters and refers to the camp being "on the soil of Kandahar" - a city in southern Afghanistan.

The father of Mohammed Atta does not believe the video is authentic. "The video-testament of my son is false and I continue to believe he is

innocent," said Muhammad al-Amir al-Sayd Atta, 71. He also believes the Americans "tampered with" and "falsified the video."

Al Jazeera said the tape was made during the planning stage of 9/11. It refused to reveal how it acquired the material though it was produced by As-Sahab, al-Qaida's so-called 'media branch'.

SPY MOSCOW

Russia targets academics and MI6 'helpers' in espionage squeeze

In August 2006, a Moscow court sentenced 42-year-old Andrei Dumenkov, a Russian scientist to 12 years in prison for trying to pass information on new rocket technology to German agents, a federal security official said.

Dumenkov pleaded guilty to charges of "high treason in the form of espionage".

FSB agents detained Dumenkov on 3 August 2005, at a Moscow railway station and claimed he had intended to flee the country once

the secrets had been passed to German agents.

The incident is the latest in a series of espionage cases investigated by Russia's FSB - the main successor agency to the Soviet-era KGB. Just weeks earlier a military court sentenced a retired Russian colonel who reportedly helped British intelligence unmask dozens of Russian agents to 13 years in prison. In January Moscow accused four British diplomats of espionage and alleged they received secret information from a radio transmitter hidden in a rock.



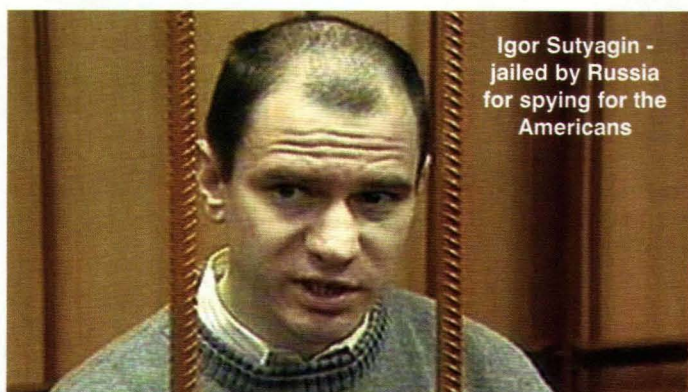
Dumenkov was detained at Kursk station in Moscow

Britain's Foreign Office refused to confirm or negate the men were MI6 officers. The country has also been embroiled in a spy row with neighbouring Georgia.

Perhaps the most famous case involving an academic is that of

Igor Sutyagin. He was sentenced to 15 years in prison for spying for the United States. The Supreme Court of Russia upheld the sentence against the scientist in April 2004. Few intelligence watchers believe he is guilty.

According to 'Human rights' advocates, the FSB is increasingly targeting Russian scientists and academics for alleged espionage or misuse of classified information. "Moscow is deeply suspicious of Russian scientists' contacts with foreigners," said one official.



Igor Sutyagin - jailed by Russia for spying for the Americans

[MI5, not nine to five]

[spooks]

behind the scenes

BBC

Available from
Eye Spy

Ref: 1126
£19.99 \$45.00

EYE SPY

INTELLIGENCE MAGAZINE

SUBSCRIBE

*using the
world's most
informed
Intel sources*

UNITED KINGDOM, USA, EUROPE, ROW

I WOULD LIKE TO SUBSCRIBE TO EYE SPY (8 ISSUES A YEAR) - PLEASE TICK APPROPRIATE BOX

UK £25.00 ☐

USA \$48.00 ☐

EUROPE/ROW £30.00 ☐

Name: _____ Address: _____

Post/Zip Code: _____ Country: _____

email: _____

Please make your cheque or money order payable to: 'EYE SPY PUBLISHING LTD' -

NOTE: WE ONLY ACCEPT UK, USA AND CANADIAN CHEQUES/POSTAL ORDERS

I enclose Cheque/Postal Order for: _____ / _____



For credit card payment by Visa, MasterCard, Switch

Credit Card No: _____

Expiry Date: _____ Three Digit Security Number (the last three numbers on the

reverse of the credit card: _____ Switch Issue No. (UK only): _____

PAYPAL eyespy@eyespy.com **ONLINE** www.eyespy.com



UK, EUROPE, ROW

Send your subscription to:

Eye Spy Publishing Ltd

P O Box 10, Skipton, North Yorkshire,
BD23 5US, UK



UNITED STATES OF AMERICA, CANADA

Mail your subscription to:

Eye Spy International

Empire State Building, 350 Fifth Ave,
Suite 3304-22H,
New York, NY 10118-0069, USA

By Telephone 01756 770199
10.00am - 5.00pm, (Mon-Fri)



TOLL FREE 7.00am - 4.00pm,
Mon-Fri 1-877-309-9243

DO/ES444

COMPL

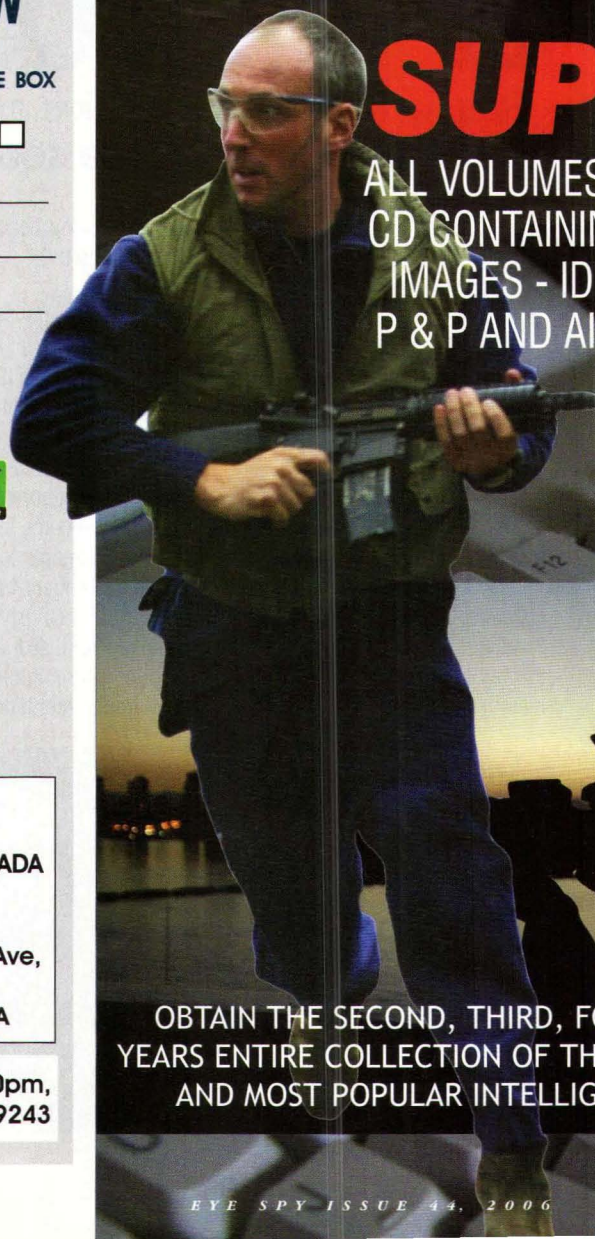
EYE SPY IN

VOLUME 2 COMPLETE

Volume II
Ref: ESVOL2
UK £35.00
USA \$60.00
ROW £40.00

SUP

ALL VOLUMES
CD CONTAINING
IMAGES - ID
P & P AND ALL



OBTAIN THE SECOND, THIRD, FOURTH, FIFTH, SIXTH, SEVENTH, EIGHTH, NINTH, TENTH, ELEVENTH, TWELFTH, THIRTEENTH, FOURTEENTH, FIFTEENTH, SIXTEENTH, SEVENTEENTH, EIGHTEENTH, NINETEENTH, TWENTIETH, TWENTY-FIRST, TWENTY-SECOND, TWENTY-THIRD, TWENTY-FOURTH, TWENTY-FIFTH, TWENTY-SIXTH, TWENTY-SEVENTH, TWENTY-EIGHTH, TWENTY-NINTH, THIRTIETH, THIRTY-FIRST, THIRTY-SECOND, THIRTY-THIRD, THIRTY-FOURTH, THIRTY-FIFTH, THIRTY-SIXTH, THIRTY-SEVENTH, THIRTY-EIGHTH, THIRTY-NINTH, FORTIETH, FORTY-FIRST, FORTY-SECOND, FORTY-THIRD, FORTY-FOURTH, FORTY-FIFTH, FORTY-SIXTH, FORTY-SEVENTH, FORTY-EIGHTH, FORTY-NINTH, FIFTIETH, FIFTY-FIRST, FIFTY-SECOND, FIFTY-THIRD, FIFTY-FOURTH, FIFTY-FIFTH, FIFTY-SIXTH, FIFTY-SEVENTH, FIFTY-EIGHTH, FIFTY-NINTH, SIXTIETH, SIXTY-FIRST, SIXTY-SECOND, SIXTY-THIRD, SIXTY-FOURTH, SIXTY-FIFTH, SIXTY-SIXTH, SIXTY-SEVENTH, SIXTY-EIGHTH, SIXTY-NINTH, SEVENTIETH, SEVENTY-FIRST, SEVENTY-SECOND, SEVENTY-THIRD, SEVENTY-FOURTH, SEVENTY-FIFTH, SEVENTY-SIXTH, SEVENTY-SEVENTH, SEVENTY-EIGHTH, SEVENTY-NINTH, EIGHTIETH, EIGHTY-FIRST, EIGHTY-SECOND, EIGHTY-THIRD, EIGHTY-FOURTH, EIGHTY-FIFTH, EIGHTY-SIXTH, EIGHTY-SEVENTH, EIGHTY-EIGHTH, EIGHTY-NINTH, NINETYETH, NINETY-FIRST, NINETY-SECOND, NINETY-THIRD, NINETY-FOURTH, NINETY-FIFTH, NINETY-SIXTH, NINETY-SEVENTH, NINETY-EIGHTH, NINETY-NINTH, ONE HUNDREDTH, ONE HUNDRED-FIRST, ONE HUNDRED-SECOND, ONE HUNDRED-THIRD, ONE HUNDRED-FOURTH, ONE HUNDRED-FIFTH, ONE HUNDRED-SIXTH, ONE HUNDRED-SEVENTH, ONE HUNDRED-EIGHTH, ONE HUNDRED-NINTH, TWO HUNDREDTH, TWO HUNDRED-FIRST, TWO HUNDRED-SECOND, TWO HUNDRED-THIRD, TWO HUNDRED-FOURTH, TWO HUNDRED-FIFTH, TWO HUNDRED-SIXTH, TWO HUNDRED-SEVENTH, TWO HUNDRED-EIGHTH, TWO HUNDRED-NINTH, THREE HUNDREDTH, THREE HUNDRED-FIRST, THREE HUNDRED-SECOND, THREE HUNDRED-THIRD, THREE HUNDRED-FOURTH, THREE HUNDRED-FIFTH, THREE HUNDRED-SIXTH, THREE HUNDRED-SEVENTH, THREE HUNDRED-EIGHTH, THREE HUNDRED-NINTH, FOUR HUNDREDTH, FOUR HUNDRED-FIRST, FOUR HUNDRED-SECOND, FOUR HUNDRED-THIRD, FOUR HUNDRED-FOURTH, FOUR HUNDRED-FIFTH, FOUR HUNDRED-SIXTH, FOUR HUNDRED-SEVENTH, FOUR HUNDRED-EIGHTH, FOUR HUNDRED-NINTH, FIVE HUNDREDTH, FIVE HUNDRED-FIRST, FIVE HUNDRED-SECOND, FIVE HUNDRED-THIRD, FIVE HUNDRED-FOURTH, FIVE HUNDRED-FIFTH, FIVE HUNDRED-SIXTH, FIVE HUNDRED-SEVENTH, FIVE HUNDRED-EIGHTH, FIVE HUNDRED-NINTH, SIX HUNDREDTH, SIX HUNDRED-FIRST, SIX HUNDRED-SECOND, SIX HUNDRED-THIRD, SIX HUNDRED-FOURTH, SIX HUNDRED-FIFTH, SIX HUNDRED-SIXTH, SIX HUNDRED-SEVENTH, SIX HUNDRED-EIGHTH, SIX HUNDRED-NINTH, SEVEN HUNDREDTH, SEVEN HUNDRED-FIRST, SEVEN HUNDRED-SECOND, SEVEN HUNDRED-THIRD, SEVEN HUNDRED-FOURTH, SEVEN HUNDRED-FIFTH, SEVEN HUNDRED-SIXTH, SEVEN HUNDRED-SEVENTH, SEVEN HUNDRED-EIGHTH, SEVEN HUNDRED-NINTH, EIGHT HUNDREDTH, EIGHT HUNDRED-FIRST, EIGHT HUNDRED-SECOND, EIGHT HUNDRED-THIRD, EIGHT HUNDRED-FOURTH, EIGHT HUNDRED-FIFTH, EIGHT HUNDRED-SIXTH, EIGHT HUNDRED-SEVENTH, EIGHT HUNDRED-EIGHTH, EIGHT HUNDRED-NINTH, NINE HUNDREDTH, NINE HUNDRED-FIRST, NINE HUNDRED-SECOND, NINE HUNDRED-THIRD, NINE HUNDRED-FOURTH, NINE HUNDRED-FIFTH, NINE HUNDRED-SIXTH, NINE HUNDRED-SEVENTH, NINE HUNDRED-EIGHTH, NINE HUNDRED-NINTH, TEN HUNDREDTH, TEN HUNDRED-FIRST, TEN HUNDRED-SECOND, TEN HUNDRED-THIRD, TEN HUNDRED-FOURTH, TEN HUNDRED-FIFTH, TEN HUNDRED-SIXTH, TEN HUNDRED-SEVENTH, TEN HUNDRED-EIGHTH, TEN HUNDRED-NINTH, ELEVEN HUNDREDTH, ELEVEN HUNDRED-FIRST, ELEVEN HUNDRED-SECOND, ELEVEN HUNDRED-THIRD, ELEVEN HUNDRED-FOURTH, ELEVEN HUNDRED-FIFTH, ELEVEN HUNDRED-SIXTH, ELEVEN HUNDRED-SEVENTH, ELEVEN HUNDRED-EIGHTH, ELEVEN HUNDRED-NINTH, TWELVE HUNDREDTH, TWELVE HUNDRED-FIRST, TWELVE HUNDRED-SECOND, TWELVE HUNDRED-THIRD, TWELVE HUNDRED-FOURTH, TWELVE HUNDRED-FIFTH, TWELVE HUNDRED-SIXTH, TWELVE HUNDRED-SEVENTH, TWELVE HUNDRED-EIGHTH, TWELVE HUNDRED-NINTH, THIRTEEN HUNDREDTH, THIRTEEN HUNDRED-FIRST, THIRTEEN HUNDRED-SECOND, THIRTEEN HUNDRED-THIRD, THIRTEEN HUNDRED-FOURTH, THIRTEEN HUNDRED-FIFTH, THIRTEEN HUNDRED-SIXTH, THIRTEEN HUNDRED-SEVENTH, THIRTEEN HUNDRED-EIGHTH, THIRTEEN HUNDRED-NINTH, FOURTEEN HUNDREDTH, FOURTEEN HUNDRED-FIRST, FOURTEEN HUNDRED-SECOND, FOURTEEN HUNDRED-THIRD, FOURTEEN HUNDRED-FOURTH, FOURTEEN HUNDRED-FIFTH, FOURTEEN HUNDRED-SIXTH, FOURTEEN HUNDRED-SEVENTH, FOURTEEN HUNDRED-EIGHTH, FOURTEEN HUNDRED-NINTH, FIFTEEN HUNDREDTH, FIFTEEN HUNDRED-FIRST, FIFTEEN HUNDRED-SECOND, FIFTEEN HUNDRED-THIRD, FIFTEEN HUNDRED-FOURTH, FIFTEEN HUNDRED-FIFTH, FIFTEEN HUNDRED-SIXTH, FIFTEEN HUNDRED-SEVENTH, FIFTEEN HUNDRED-EIGHTH, FIFTEEN HUNDRED-NINTH, SIXTEEN HUNDREDTH, SIXTEEN HUNDRED-FIRST, SIXTEEN HUNDRED-SECOND, SIXTEEN HUNDRED-THIRD, SIXTEEN HUNDRED-FOURTH, SIXTEEN HUNDRED-FIFTH, SIXTEEN HUNDRED-SIXTH, SIXTEEN HUNDRED-SEVENTH, SIXTEEN HUNDRED-EIGHTH, SIXTEEN HUNDRED-NINTH, SEVENTEEN HUNDREDTH, SEVENTEEN HUNDRED-FIRST, SEVENTEEN HUNDRED-SECOND, SEVENTEEN HUNDRED-THIRD, SEVENTEEN HUNDRED-FOURTH, SEVENTEEN HUNDRED-FIFTH, SEVENTEEN HUNDRED-SIXTH, SEVENTEEN HUNDRED-SEVENTH, SEVENTEEN HUNDRED-EIGHTH, SEVENTEEN HUNDRED-NINTH, EIGHTEEN HUNDREDTH, EIGHTEEN HUNDRED-FIRST, EIGHTEEN HUNDRED-SECOND, EIGHTEEN HUNDRED-THIRD, EIGHTEEN HUNDRED-FOURTH, EIGHTEEN HUNDRED-FIFTH, EIGHTEEN HUNDRED-SIXTH, EIGHTEEN HUNDRED-SEVENTH, EIGHTEEN HUNDRED-EIGHTH, EIGHTEEN HUNDRED-NINTH, NINETEEN HUNDREDTH, NINETEEN HUNDRED-FIRST, NINETEEN HUNDRED-SECOND, NINETEEN HUNDRED-THIRD, NINETEEN HUNDRED-FOURTH, NINETEEN HUNDRED-FIFTH, NINETEEN HUNDRED-SIXTH, NINETEEN HUNDRED-SEVENTH, NINETEEN HUNDRED-EIGHTH, NINETEEN HUNDRED-NINTH, TWENTY HUNDREDTH, TWENTY HUNDRED-FIRST, TWENTY HUNDRED-SECOND, TWENTY HUNDRED-THIRD, TWENTY HUNDRED-FOURTH, TWENTY HUNDRED-FIFTH, TWENTY HUNDRED-SIXTH, TWENTY HUNDRED-SEVENTH, TWENTY HUNDRED-EIGHTH, TWENTY HUNDRED-NINTH, TWENTY-ONE HUNDREDTH, TWENTY-ONE HUNDRED-FIRST, TWENTY-ONE HUNDRED-SECOND, TWENTY-ONE HUNDRED-THIRD, TWENTY-ONE HUNDRED-FOURTH, TWENTY-ONE HUNDRED-FIFTH, TWENTY-ONE HUNDRED-SIXTH, TWENTY-ONE HUNDRED-SEVENTH, TWENTY-ONE HUNDRED-EIGHTH, TWENTY-ONE HUNDRED-NINTH, TWENTY-TWO HUNDREDTH, TWENTY-TWO HUNDRED-FIRST, TWENTY-TWO HUNDRED-SECOND, TWENTY-TWO HUNDRED-THIRD, TWENTY-TWO HUNDRED-FOURTH, TWENTY-TWO HUNDRED-FIFTH, TWENTY-TWO HUNDRED-SIXTH, TWENTY-TWO HUNDRED-SEVENTH, TWENTY-TWO HUNDRED-EIGHTH, TWENTY-TWO HUNDRED-NINTH, TWENTY-THREE HUNDREDTH, TWENTY-THREE HUNDRED-FIRST, TWENTY-THREE HUNDRED-SECOND, TWENTY-THREE HUNDRED-THIRD, TWENTY-THREE HUNDRED-FOURTH, TWENTY-THREE HUNDRED-FIFTH, TWENTY-THREE HUNDRED-SIXTH, TWENTY-THREE HUNDRED-SEVENTH, TWENTY-THREE HUNDRED-EIGHTH, TWENTY-THREE HUNDRED-NINTH, TWENTY-FOUR HUNDREDTH, TWENTY-FOUR HUNDRED-FIRST, TWENTY-FOUR HUNDRED-SECOND, TWENTY-FOUR HUNDRED-THIRD, TWENTY-FOUR HUNDRED-FOURTH, TWENTY-FOUR HUNDRED-FIFTH, TWENTY-FOUR HUNDRED-SIXTH, TWENTY-FOUR HUNDRED-SEVENTH, TWENTY-FOUR HUNDRED-EIGHTH, TWENTY-FOUR HUNDRED-NINTH, TWENTY-FIVE HUNDREDTH, TWENTY-FIVE HUNDRED-FIRST, TWENTY-FIVE HUNDRED-SECOND, TWENTY-FIVE HUNDRED-THIRD, TWENTY-FIVE HUNDRED-FOURTH, TWENTY-FIVE HUNDRED-FIFTH, TWENTY-FIVE HUNDRED-SIXTH, TWENTY-FIVE HUNDRED-SEVENTH, TWENTY-FIVE HUNDRED-EIGHTH, TWENTY-FIVE HUNDRED-NINTH, TWENTY-SIX HUNDREDTH, TWENTY-SIX HUNDRED-FIRST, TWENTY-SIX HUNDRED-SECOND, TWENTY-SIX HUNDRED-THIRD, TWENTY-SIX HUNDRED-FOURTH, TWENTY-SIX HUNDRED-FIFTH, TWENTY-SIX HUNDRED-SIXTH, TWENTY-SIX HUNDRED-SEVENTH, TWENTY-SIX HUNDRED-EIGHTH, TWENTY-SIX HUNDRED-NINTH, TWENTY-SEVEN HUNDREDTH, TWENTY-SEVEN HUNDRED-FIRST, TWENTY-SEVEN HUNDRED-SECOND, TWENTY-SEVEN HUNDRED-THIRD, TWENTY-SEVEN HUNDRED-FOURTH, TWENTY-SEVEN HUNDRED-FIFTH, TWENTY-SEVEN HUNDRED-SIXTH, TWENTY-SEVEN HUNDRED-SEVENTH, TWENTY-SEVEN HUNDRED-EIGHTH, TWENTY-SEVEN HUNDRED-NINTH, TWENTY-EIGHT HUNDREDTH, TWENTY-EIGHT HUNDRED-FIRST, TWENTY-EIGHT HUNDRED-SECOND, TWENTY-EIGHT HUNDRED-THIRD, TWENTY-EIGHT HUNDRED-FOURTH, TWENTY-EIGHT HUNDRED-FIFTH, TWENTY-EIGHT HUNDRED-SIXTH, TWENTY-EIGHT HUNDRED-SEVENTH, TWENTY-EIGHT HUNDRED-EIGHTH, TWENTY-EIGHT HUNDRED-NINTH, TWENTY-NINE HUNDREDTH, TWENTY-NINE HUNDRED-FIRST, TWENTY-NINE HUNDRED-SECOND, TWENTY-NINE HUNDRED-THIRD, TWENTY-NINE HUNDRED-FOURTH, TWENTY-NINE HUNDRED-FIFTH, TWENTY-NINE HUNDRED-SIXTH, TWENTY-NINE HUNDRED-SEVENTH, TWENTY-NINE HUNDRED-EIGHTH, TWENTY-NINE HUNDRED-NINTH, THIRTY HUNDREDTH, THIRTY HUNDRED-FIRST, THIRTY HUNDRED-SECOND, THIRTY HUNDRED-THIRD, THIRTY HUNDRED-FOURTH, THIRTY HUNDRED-FIFTH, THIRTY HUNDRED-SIXTH, THIRTY HUNDRED-SEVENTH, THIRTY HUNDRED-EIGHTH, THIRTY HUNDRED-NINTH, THIRTY-ONE HUNDREDTH, THIRTY-ONE HUNDRED-FIRST, THIRTY-ONE HUNDRED-SECOND, THIRTY-ONE HUNDRED-THIRD, THIRTY-ONE HUNDRED-FOURTH, THIRTY-ONE HUNDRED-FIFTH, THIRTY-ONE HUNDRED-SIXTH, THIRTY-ONE HUNDRED-SEVENTH, THIRTY-ONE HUNDRED-EIGHTH, THIRTY-ONE HUNDRED-NINTH, THIRTY-TWO HUNDREDTH, THIRTY-TWO HUNDRED-FIRST, THIRTY-TWO HUNDRED-SECOND, THIRTY-TWO HUNDRED-THIRD, THIRTY-TWO HUNDRED-FOURTH, THIRTY-TWO HUNDRED-FIFTH, THIRTY-TWO HUNDRED-SIXTH, THIRTY-TWO HUNDRED-SEVENTH, THIRTY-TWO HUNDRED-EIGHTH, THIRTY-TWO HUNDRED-NINTH, THIRTY-THREE HUNDREDTH, THIRTY-THREE HUNDRED-FIRST, THIRTY-THREE HUNDRED-SECOND, THIRTY-THREE HUNDRED-THIRD, THIRTY-THREE HUNDRED-FOURTH, THIRTY-THREE HUNDRED-FIFTH, THIRTY-THREE HUNDRED-SIXTH, THIRTY-THREE HUNDRED-SEVENTH, THIRTY-THREE HUNDRED-EIGHTH, THIRTY-THREE HUNDRED-NINTH, THIRTY-FOUR HUNDREDTH, THIRTY-FOUR HUNDRED-FIRST, THIRTY-FOUR HUNDRED-SECOND, THIRTY-FOUR HUNDRED-THIRD, THIRTY-FOUR HUNDRED-FOURTH, THIRTY-FOUR HUNDRED-FIFTH, THIRTY-FOUR HUNDRED-SIXTH, THIRTY-FOUR HUNDRED-SEVENTH, THIRTY-FOUR HUNDRED-EIGHTH, THIRTY-FOUR HUNDRED-NINTH, THIRTY-FIVE HUNDREDTH, THIRTY-FIVE HUNDRED-FIRST, THIRTY-FIVE HUNDRED-SECOND, THIRTY-FIVE HUNDRED-THIRD, THIRTY-FIVE HUNDRED-FOURTH, THIRTY-FIVE HUNDRED-FIFTH, THIRTY-FIVE HUNDRED-SIXTH, THIRTY-FIVE HUNDRED-SEVENTH, THIRTY-FIVE HUNDRED-EIGHTH, THIRTY-FIVE HUNDRED-NINTH, THIRTY-SIX HUNDREDTH, THIRTY-SIX HUNDRED-FIRST, THIRTY-SIX HUNDRED-SECOND, THIRTY-SIX HUNDRED-THIRD, THIRTY-SIX HUNDRED-FOURTH, THIRTY-SIX HUNDRED-FIFTH, THIRTY-SIX HUNDRED-SIXTH, THIRTY-SIX HUNDRED-SEVENTH, THIRTY-SIX HUNDRED-EIGHTH, THIRTY-SIX HUNDRED-NINTH, THIRTY-SEVEN HUNDREDTH, THIRTY-SEVEN HUNDRED-FIRST, THIRTY-SEVEN HUNDRED-SECOND, THIRTY-SEVEN HUNDRED-THIRD, THIRTY-SEVEN HUNDRED-FOURTH, THIRTY-SEVEN HUNDRED-FIFTH, THIRTY-SEVEN HUNDRED-SIXTH, THIRTY-SEVEN HUNDRED-SEVENTH, THIRTY-SEVEN HUNDRED-EIGHTH, THIRTY-SEVEN HUNDRED-NINTH, THIRTY-EIGHT HUNDREDTH, THIRTY-EIGHT HUNDRED-FIRST, THIRTY-EIGHT HUNDRED-SECOND, THIRTY-EIGHT HUNDRED-THIRD, THIRTY-EIGHT HUNDRED-FOURTH, THIRTY-EIGHT HUNDRED-FIFTH, THIRTY-EIGHT HUNDRED-SIXTH, THIRTY-EIGHT HUNDRED-SEVENTH, THIRTY-EIGHT HUNDRED-EIGHTH, THIRTY-EIGHT HUNDRED-NINTH, THIRTY-NINE HUNDREDTH, THIRTY-NINE HUNDRED-FIRST, THIRTY-NINE HUNDRED-SECOND, THIRTY-NINE HUNDRED-THIRD, THIRTY-NINE HUNDRED-FOURTH, THIRTY-NINE HUNDRED-FIFTH, THIRTY-NINE HUNDRED-SIXTH, THIRTY-NINE HUNDRED-SEVENTH, THIRTY-NINE HUNDRED-EIGHTH, THIRTY-NINE HUNDRED-NINTH, FORTY HUNDREDTH, FORTY HUNDRED-FIRST, FORTY HUNDRED-SECOND, FORTY HUNDRED-THIRD, FORTY HUNDRED-FOURTH, FORTY HUNDRED-FIFTH, FORTY HUNDRED-SIXTH, FORTY HUNDRED-SEVENTH, FORTY HUNDRED-EIGHTH, FORTY HUNDRED-NINTH, FORTY-ONE HUNDREDTH, FORTY-ONE HUNDRED-FIRST, FORTY-ONE HUNDRED-SECOND, FORTY-ONE HUNDRED-THIRD, FORTY-ONE HUNDRED-FOURTH, FORTY-ONE HUNDRED-FIFTH, FORTY-ONE HUNDRED-SIXTH, FORTY-ONE HUNDRED-SEVENTH, FORTY-ONE HUNDRED-EIGHTH, FORTY-ONE HUNDRED-NINTH, FORTY-TWO HUNDREDTH, FORTY-TWO HUNDRED-FIRST, FORTY-TWO HUNDRED-SECOND, FORTY-TWO HUNDRED-THIRD, FORTY-TWO HUNDRED-FOURTH, FORTY-TWO HUNDRED-FIFTH, FORTY-TWO HUNDRED-SIXTH, FORTY-TWO HUNDRED-SEVENTH, FORTY-TWO HUNDRED-EIGHTH, FORTY-TWO HUNDRED-NINTH, FORTY-THREE HUNDREDTH, FORTY-THREE HUNDRED-FIRST, FORTY-THREE HUNDRED-SECOND, FORTY-THREE HUNDRED-THIRD, FORTY-THREE HUNDRED-FOURTH, FORTY-THREE HUNDRED-FIFTH, FORTY-THREE HUNDRED-SIXTH, FORTY-THREE HUNDRED-SEVENTH, FORTY-THREE HUNDRED-EIGHTH, FORTY-THREE HUNDRED-NINTH, FORTY-FOUR HUNDREDTH, FORTY-FOUR HUNDRED-FIRST, FORTY-FOUR HUNDRED-SECOND, FORTY-FOUR HUNDRED-THIRD, FORTY-FOUR HUNDRED-FOURTH, FORTY-FOUR HUNDRED-FIFTH, FORTY-FOUR HUNDRED-SIXTH, FORTY-FOUR HUNDRED-SEVENTH, FORTY-FOUR HUNDRED-EIGHTH, FORTY-FOUR HUNDRED-NINTH, FORTY-FIVE HUNDREDTH, FORTY-FIVE HUNDRED-FIRST, FORTY-FIVE HUNDRED-SECOND, FORTY-FIVE HUNDRED-THIRD, FORTY-FIVE HUNDRED-FOURTH, FORTY-FIVE HUNDRED-FIFTH, FORTY-FIVE HUNDRED-SIXTH, FORTY-FIVE HUNDRED-SEVENTH, FORTY-FIVE HUNDRED-EIGHTH, FORTY-FIVE HUNDRED-NINTH, FORTY-SIX HUNDREDTH, FORTY-SIX HUNDRED-FIRST, FORTY-SIX HUNDRED-SECOND, FORTY-SIX HUNDRED-THIRD, FORTY-SIX HUNDRED-FOURTH, FORTY-SIX HUNDRED-FIFTH, FORTY-SIX HUNDRED-SIXTH, FORTY-SIX HUNDRED-SEVENTH, FORTY-SIX HUNDRED-EIGHTH, FORTY-SIX HUNDRED-NINTH, FORTY-SEVEN HUNDREDTH, FORTY-SEVEN HUNDRED-FIRST, FORTY-SEVEN HUNDRED-SECOND, FORTY-SEVEN HUNDRED-THIRD, FORTY-SEVEN HUNDRED-FOURTH, FORTY-SEVEN HUNDRED-FIFTH, FORTY-SEVEN HUNDRED-SIXTH, FORTY-SEVEN HUNDRED-SEVENTH, FORTY-SEVEN HUNDRED-EIGHTH, FORTY-SEVEN HUNDRED-NINTH, FORTY-EIGHT HUNDREDTH, FORTY-EIGHT HUNDRED-FIRST, FORTY-EIGHT HUNDRED-SECOND, FORTY-EIGHT HUNDRED-THIRD, FORTY-EIGHT HUNDRED-FOURTH, FORTY-EIGHT HUNDRED-FIFTH, FORTY-EIGHT HUNDRED-SIXTH, FORTY-EIGHT HUNDRED-SEVENTH, FORTY-EIGHT HUNDRED-EIGHTH, FORTY-EIGHT HUNDRED-NINTH, FORTY-NINE HUNDREDTH, FORTY-NINE HUNDRED-FIRST, FORTY-NINE HUNDRED-SECOND, FORTY-NINE HUNDRED-THIRD, FORTY-NINE HUNDRED-FOURTH, FORTY-NINE HUNDRED-FIFTH, FORTY-NINE HUNDRED-SIXTH, FORTY-NINE HUNDRED-SEVENTH, FORTY-NINE HUNDRED-EIGHTH, FORTY-NINE HUNDRED-NINTH, FIFTY HUNDREDTH, FIFTY HUNDRED-FIRST, FIFTY HUNDRED-SECOND, FIFTY HUNDRED-THIRD, FIFTY HUNDRED-FOURTH, FIFTY HUNDRED-FIFTH, FIFTY HUNDRED-SIXTH, FIFTY HUNDRED-SEVENTH, FIFTY HUNDRED-EIGHTH, FIFTY HUNDRED-NINTH, FIFTY-ONE HUNDREDTH, FIFTY-ONE HUNDRED-FIRST, FIFTY-ONE HUNDRED-SECOND, FIFTY-ONE HUNDRED-THIRD, FIFTY-ONE HUNDRED-FOURTH, FIFTY-ONE HUNDRED-FIFTH, FIFTY-ONE HUNDRED-SIXTH, FIFTY-ONE HUNDRED-SEVENTH, FIFTY-ONE HUNDRED-EIGHTH, FIFTY-ONE HUNDRED-NINTH, FIFTY-TWO HUNDREDTH, FIFTY-TWO HUNDRED-FIRST, FIFTY-TWO HUNDRED-SECOND, FIFTY-TWO HUNDRED-THIRD, FIFTY-TWO HUNDRED-FOURTH, FIFTY-TWO HUNDRED-FIFTH, FIFTY-TWO HUNDRED-SIXTH, FIFTY-TWO HUNDRED-SEVENTH, FIFTY-TWO HUNDRED-EIGHTH, FIFTY-TWO HUNDRED-NINTH, FIFTY-THREE HUNDREDTH, FIFTY-THREE HUNDRED-FIRST, FIFTY-THREE HUNDRED-SECOND, FIFTY-THREE HUNDRED-THIRD, FIFTY-THREE HUNDRED-FOURTH, FIFTY-THREE HUNDRED-FIFTH, FIFTY-THREE HUNDRED-SIXTH, FIFTY-THREE HUNDRED-SEVENTH, FIFTY-THREE HUNDRED-EIGHTH, FIFTY-THREE HUNDRED-NINTH, FIFTY-FOUR HUNDREDTH, FIFTY-FOUR HUNDRED-FIRST, FIFTY-FOUR HUNDRED-SECOND, FIFTY-FOUR HUNDRED-THIRD, FIFTY-FOUR HUNDRED-FOURTH, FIFTY-FOUR HUNDRED-FIFTH, FIFTY-FOUR HUNDRED-SIXTH, FIFTY-FOUR HUNDRED-SEVENTH, FIFTY-FOUR HUNDRED-EIGHTH, FIFTY-FOUR HUNDRED-NINTH, FIFTY-FIVE HUNDREDTH, FIFTY-FIVE HUNDRED-FIRST, FIFTY-FIVE HUNDRED-SECOND, FIFTY-FIVE HUNDRED-THIRD, FIFTY-FIVE HUNDRED-FOURTH, FIFTY-FIVE HUNDRED-FIFTH, FIFTY-FIVE HUNDRED-SIXTH, FIFTY-FIVE HUNDRED-SEVENTH, FIFTY-FIVE HUNDRED-EIGHTH, FIFTY-FIVE HUNDRED-NINTH, FIFTY-SIX HUNDREDTH, FIFTY-SIX HUNDRED-FIRST, FIFTY-SIX HUNDRED-SECOND, FIFTY-SIX HUNDRED-THIRD, FIFTY-SIX HUNDRED-FOURTH, FIFTY-SIX HUNDRED-FIFTH, FIFTY-SIX HUNDRED-SIXTH, FIFTY-SIX HUNDRED-SEVENTH, FIFTY-SIX HUNDRED-EIGHTH, FIFTY-SIX HUNDRED-NINTH, FIFTY-SEVEN HUNDREDTH, FIFTY-SEVEN HUNDRED-FIRST, FIFTY-SEVEN HUNDRED-SECOND, FIFTY-SEVEN HUNDRED-THIRD, FIFTY-SEVEN HUNDRED-FOURTH, FIFTY-SEVEN HUNDRED-FIFTH, FIFTY-SEVEN HUNDRED-SIXTH, FIFTY-SEVEN HUNDRED-SEVENTH, FIFTY-SEVEN HUNDRED-EIGHTH, FIFTY-SEVEN HUNDRED-NINTH, FIFTY-EIGHT HUNDREDTH, FIFTY-EIGHT HUNDRED-FIRST, FIFTY-EIGHT HUNDRED-SECOND, FIFTY-EIGHT HUNDRED-THIRD, FIFTY-EIGHT HUNDRED-FOURTH, FIFTY-EIGHT HUNDRED-FIFTH, FIFTY-EIGHT HUNDRED-SIXTH, FIFTY-EIGHT HUNDRED-SEVENTH, FIFTY-EIGHT HUNDRED-EIGHTH, FIFTY-EIGHT HUNDRED-NINTH, FIFTY-NINE HUNDREDTH, FIFTY-NINE HUNDRED-FIRST, FIFTY-NINE HUNDRED-SECOND, FIFTY-NINE HUNDRED-THIRD, FIFTY-NINE HUNDRED-FOURTH, FIFTY-NINE HUNDRED-FIFTH, FIFTY-NINE HUNDRED-SIXTH, FIFTY-NINE HUNDRED-SEVENTH, FIFTY-NINE HUNDRED-EIGHTH, FIFTY-NINE HUNDRED-NINTH, SIXTY HUNDREDTH, SIXTY HUNDRED-FIRST, SIXTY HUNDRED-SECOND, SIXTY HUNDRED-THIRD, SIXTY HUNDRED-FOURTH, SIXTY HUNDRED-FIFTH, SIXTY HUNDRED-SIXTH, SIXTY HUNDRED-SEVENTH, SIXTY HUNDRED-EIGHTH, SIXTY HUNDRED-NINTH, SIXTY-ONE HUNDREDTH, SIXTY-ONE HUNDRED-FIRST, SIXTY-ONE HUNDRED-SECOND, SIXTY-ONE HUNDRED-THIRD, SIXTY-ONE HUNDRED-FOURTH, SIXTY-ONE HUNDRED-FIFTH, SIXTY-ONE HUNDRED-SIXTH, SIXTY-ONE HUNDRED-SEVENTH, SIXTY-ONE HUNDRED-EIGHTH, SIXTY-ONE HUNDRED-NINTH, SIXTY-TWO HUNDREDTH, SIXTY-TWO HUNDRED-FIRST, SIXTY-TWO HUNDRED-SECOND, SIXTY-TWO HUNDRED-THIRD, SIXTY-TWO HUNDRED-FOURTH, SIXTY-TWO HUNDRED-FIFTH, SIXTY-TWO HUNDRED-SIXTH, SIXTY-TWO HUNDRED-SEVENTH, SIXTY-TWO HUNDRED-EIGHTH, SIXTY-TWO HUNDRED-NINTH, SIXTY-THREE HUNDREDTH, SIXTY-THREE HUNDRED-FIRST, SIXTY-THREE HUNDRED-SECOND, SIXTY-THREE HUNDRED-THIRD, SIXTY-THREE HUNDRED-FOURTH, SIXTY-THREE HUNDRED-FIFTH, SIXTY-THREE HUNDRED-SIXTH, SIXTY-THREE HUNDRED-SEVENTH, SIXTY-THREE HUNDRED-EIGHTH, SIXTY-THREE HUNDRED-NINTH, SIXTY-FOUR HUNDREDTH, SIXTY-FOUR HUNDRED-FIRST, SIXTY-FOUR HUNDRED-SECOND, SIXTY-FOUR HUNDRED-THIRD, SIXTY-FOUR HUNDRED-FOURTH, SIXTY-FOUR HUNDRED-FIFTH, SIXTY-FOUR HUNDRED-SIXTH, SIXTY-FOUR HUNDRED-SEVENTH, SIXTY-FOUR HUNDRED-EIGHTH, SIXTY-FOUR HUNDRED-NINTH, SIXTY-FIVE HUNDREDTH, SIXTY-FIVE HUNDRED-FIRST, SIXTY-FIVE HUNDRED-SECOND, SIXTY-FIVE HUNDRED-THIRD, SIXTY-FIVE HUNDRED-FOURTH, SIXTY-FIVE HUNDRED-FIFTH, SIXTY-FIVE HUNDRED-SIXTH, SIXTY-FIVE HUNDRED-SEVENTH, SIXTY-FIVE HUNDRED-EIGHTH, SIXTY-FIVE HUNDRED-NINTH, SIXTY-SIX HUNDREDTH, SIXTY-SIX HUNDRED-FIRST, SIXTY-SIX HUNDRED-SECOND, SIXTY-SIX HUNDRED-THIRD, SIXTY-SIX HUNDRED-FOURTH, SIXTY-SIX HUNDRED-FIFTH, SIXTY-SIX HUNDRED-SIXTH, SIXTY-SIX HUNDRED-SEVENTH, SIXTY-SIX HUNDRED-EIGHTH, SIXTY-SIX HUNDRED-NINTH, SIXTY-SEVEN HUNDREDTH, SIXTY-SEVEN HUNDRED-FIRST, SIXTY-SEVEN HUNDRED-SECOND, SIXTY-SEVEN HUNDRED-THIRD, SIXTY-SEVEN HUNDRED-FOURTH, SIXTY-SEVEN HUNDRED-FIFTH, SIXTY-SEVEN HUNDRED-SIXTH, SIXTY-SEVEN HUNDRED-SEVENTH, SIXTY-SEVEN HUNDRED-EIGHTH, SIXTY-SEVEN HUNDRED-NINTH, SIXTY-EIGHT HUNDREDTH, SIXTY-EIGHT HUNDRED-FIRST, SIXTY-EIGHT HUNDRED-SECOND, SIXTY-EIGHT HUNDRED-THIRD, SIXTY-EIGHT HUNDRED-FOURTH, SIXTY-EIGHT HUNDRED-FIFTH, SIXTY-EIGHT HUNDRED-SIXTH, SIXTY-EIGHT HUNDRED-SEVENTH, SIXTY-EIGHT HUNDRED-EIGHTH, SIXTY-EIGHT HUNDRED-NINTH, SIXTY-NINE HUNDREDTH, SIXTY-NINE HUNDRED-FIRST, SIXTY-NINE HUNDRED-SECOND, SIXTY-NINE HUNDRED-THIRD, SIXTY-NINE HUNDRED-FOURTH, SIXTY-NINE HUNDRED-FIFTH, SIXTY-NINE HUNDRED-SIXTH, SIXTY-NINE HUNDRED-SEVENTH, SIXTY-NINE HUNDRED-EIGHTH, SIXTY-NINE HUNDRED-NINTH, SEVENTY HUNDREDTH, SEVENTY HUNDRED-FIRST, SEVENTY HUNDRED-SECOND, SEVENTY HUNDRED-THIRD, SEVENTY HUNDRED-FOURTH, SEVENTY HUNDRED-FIFTH, SEVENTY HUNDRED-SIXTH, SEVENTY HUNDRED-SEVENTH, SEVENTY HUNDRED-EIGHTH, SEVENTY HUNDRED-NINTH, SEVENTY-ONE HUNDREDTH, SEVENTY-ONE HUNDRED-FIRST, SEVENTY-ONE HUNDRED-SECOND, SEVENTY-ONE HUNDRED-THIRD, SEVENTY-ONE HUNDRED-FOURTH, SEVENTY-ONE HUNDRED-FIFTH, SEVENTY-ONE HUNDRED-SIXTH, SEVENTY-ONE HUNDRED-SEVENTH, SEVENTY-ONE HUNDRED-EIGHTH, SEVENTY-ONE HUNDRED-NINTH, SEVENTY-TWO HUNDREDTH, SEVENTY-TWO HUNDRED-FIRST, SEVENTY-TWO HUNDRED-SECOND, SEVENTY-TWO HUNDRED-THIRD, SEVENTY-TWO HUNDRED-FOURTH, SEVENTY-TWO HUNDRED-FIFTH, SEVENTY-TWO HUNDRED-SIXTH, SEVENTY-TWO HUNDRED-SEVENTH, SEVENTY-TWO HUNDRED-EIGHTH, SEVENTY-TWO HUNDRED-NINTH, SEVENTY-THREE HUNDREDTH, SEVENTY-THREE HUNDRED-FIRST, SEVENTY-THREE HUNDRED-SECOND, SEVENTY-THREE HUNDRED-THIRD, SEVENTY-THREE HUNDRED-FOURTH, SEVENTY-THREE HUNDRED-FIFTH, SEVENTY-THREE HUNDRED-SIXTH, SEVENTY-THREE HUNDRED-SEVENTH, SEVENTY-THREE HUNDRED-EIGHTH, SEVENTY-THREE HUNDRED-NINTH, SEVENTY-FOUR HUNDREDTH, SEVENTY-FOUR HUNDRED-FIRST, SEVENTY-FOUR HUNDRED-SECOND, SEVENTY-FOUR HUNDRED-THIRD, SEVENTY-FOUR HUNDRED-FOURTH, SEVENTY-FOUR HUNDRED-FIFTH, SEVENTY-FOUR HUNDRED-SIXTH, SEVENTY-FOUR HUNDRED-SEVENTH, SEVENTY-FOUR HUNDRED-EIGHTH, SEVENTY-FOUR HUNDRED-NINTH, SEVENTY-FIVE HUNDREDTH, SEVENTY-FIVE HUNDRED-FIRST, SEVENTY-FIVE HUNDRED-SECOND, SEVENTY-FIVE HUNDRED-THIRD, SEVENTY-FIVE HUNDRED-FOURTH, SEVENTY-FIVE HUNDRED-FIFTH, SEVENTY-FIVE HUNDRED-SIXTH, SEVENTY-FIVE HUNDRED-SEVENTH, SEVENTY-FIVE HUNDRED-EIGHTH, SEVENTY-FIVE HUNDRED-NINTH, SEVENTY-SIX HUNDREDTH, SEVENTY-SIX HUNDRED-FIRST, SEVENTY-SIX HUNDRED-SECOND, SEVENTY-SIX HUNDRED-THIRD, SEVENTY-SIX HUNDRED-FOURTH, SEVENTY-SIX HUNDRED-FIFTH, SEVENTY-SIX HUNDRED-SIXTH, SEVENTY-SIX HUNDRED-SEVENTH, SEVENTY-SIX HUNDRED-EIGHTH, SEVENTY-SIX HUNDRED-NINTH, SEVENTY-SEVEN HUNDREDTH, SEVENTY-SEVEN HUNDRED-FIRST, SEVENTY-SEVEN HUNDRED-SECOND, SEVENTY-SEVEN HUNDRED-THIRD, SEVENTY-SEVEN HUNDRED-FOURTH, SEVENTY-SEVEN HUNDRED-FIFTH, SEVENTY-SEVEN HUNDRED-SIXTH, SEVENTY-SEVEN HUNDRED-SEVENTH, SEVENTY-SEVEN HUNDRED-EIGHTH, SEVENTY-SEVEN HUNDRED-NINTH, SEVENTY-EIGHT HUNDREDTH, SEVENTY-EIGHT HUNDRED-FIRST, SEVENTY-EIGHT HUNDRED-SECOND, SEVENTY-EIGHT HUNDRED-THIRD, SEVENTY-EIGHT HUNDRED-FOURTH, SEVENTY-EIGHT HUNDRED-FIFTH, SEVENTY-EIGHT HUNDRED-SIXTH, SEVENTY-EIGHT HUNDRED-SEVENTH, SEVENTY-EIGHT HUNDRED-EIGHTH, SEVENTY-EIGHT HUNDRED-NINTH, SEVENTY-NINE HUNDREDTH, SEVENTY-NINE HUNDRED-FIRST, SEVENTY-NINE HUNDRED-SECOND, SEVENTY-NINE HUNDRED-THIRD, SEVENTY-NINE HUNDRED-FOURTH, SEVENTY-NINE HUNDRED-FIFTH, SEVENTY-NINE HUNDRED-SIXTH, SEVENTY-NINE HUNDRED-SEVENTH, SEVENTY-NINE HUNDRED-EIGHTH, SEVENTY-NINE HUNDRED-NINTH, EIGHTY HUNDREDTH, EIGHTY HUNDRED-FIRST, EIGHTY HUNDRED-SECOND, EIGHTY HUNDRED-THIRD, EIGHTY HUNDRED-FOURTH, EIGHTY HUNDRED-FIFTH, EIGHTY HUNDRED-SIXTH, EIGHTY HUNDRED-SEVENTH, EIGHTY HUNDRED-EIGHTH, EIGHTY HUNDRED-NINTH, EIGHTY-ONE HUNDREDTH, EIGHTY-ONE HUNDRED-FIRST, EIGHTY-ONE HUNDRED-SECOND, EIGHTY-ONE HUNDRED-THIRD, EIGHTY-ONE HUNDRED-FOURTH, EIGHTY-ONE HUNDRED-FIFTH, EIGHTY-ONE HUNDRED-SIXTH, EIGHTY-ONE HUNDRED-SEVENTH, EIGHTY-ONE HUNDRED-EIGHTH, EIGHTY-ONE HUNDRED-NINTH, EIGHTY-TWO HUNDREDTH, EIGHTY-TWO HUNDRED-FIRST, EIGHTY-TWO HUNDRED-SECOND, EIGHTY-TWO HUNDRED-THIRD, EIGHTY-TWO HUNDRED-FOURTH, EIGHTY-TWO HUNDRED-FIFTH, EIGHTY-TWO HUNDRED-SIXTH, EIGHTY-TWO HUNDRED-SEVENTH, EIGHTY-TWO HUNDRED-EIGHTH, EIGHTY-TWO HUNDRED-NINTH, EIGHTY-THREE HUNDREDTH, EIGHTY-THREE HUNDRED-FIRST, EIGHTY-THREE HUNDRED-SECOND, EIGHTY-THREE HUNDRED-THIRD, EIGHTY-THREE HUNDRED-FOURTH, EIGHTY-THREE HUNDRED-FIFTH, EIGHTY-THREE HUNDRED-SIXTH, EIGHTY-THREE HUNDRED-SEVENTH, EIGHTY-THREE HUNDRED-EIGHTH, EIGHTY-THREE HUNDRED-NINTH, EIGHTY-FOUR HUNDREDTH, EIGHTY-FOUR HUNDRED-FIRST, EIGHTY-FOUR HUNDRED-SECOND, EIGHTY-FOUR HUNDRED-THIRD, EIGHTY-FOUR HUNDRED-FOURTH, EIGHTY-FOUR HUNDRED-FIFTH, EIGHTY-FOUR HUNDRED-SIXTH, EIGHTY-FOUR HUNDRED-SEVENTH, EIGHTY-FOUR HUNDRED-EIGHTH, EIGHTY-FOUR HUNDRED-NINTH, EIGHTY-FIVE HUNDREDTH, EIGHTY-FIVE HUNDRED-FIRST, EIGHTY-FIVE HUNDRED-SECOND, EIGHTY-FIVE HUNDRED-THIRD, EIGHTY-FIVE HUNDRED-FOURTH, EIGHTY-FIVE HUNDRED-FIFTH, EIGHTY-FIVE HUNDRED-SIXTH, EIGHTY-FIVE HUNDRED-SEVENTH, EIGHTY-FIVE HUNDRED-EIGHTH, EIGHTY-FIVE HUNDRED-NINTH, EIGHTY-SIX HUNDREDTH, EIGHTY-SIX HUNDRED-FIRST, EIGHTY-SIX HUNDRED-SECOND, EIGHTY-SIX HUNDRED-THIRD, EIGHTY-SIX HUNDRED-FOURTH, EIGHTY-SIX HUNDRED-FIFTH, EIGHTY-SIX HUNDRED-SIXTH, EIGHTY-SIX HUNDRED-SEVENTH, EIGHTY-SIX HUNDRED-EIGHTH, EIGHTY-SIX HUNDRED-NINTH, EIGHTY-SEVEN HUNDREDTH, EIGHTY-SEVEN HUNDRED-FIRST, EIGHTY-SEVEN HUNDRED-SECOND, EIGHTY-SEVEN HUNDRED-THIRD, EIGHTY-SEVEN HUNDRED-FOURTH, EIGHTY-SEVEN HUNDRED-FIFTH, EIGHTY-SEVEN HUNDRED-SIXTH, EIGHTY-SEVEN HUNDRED-SEVENTH, EIGHTY-

TE VOLUMES

LLIGENCE MAGAZINE

VOLUME COMPLETE

Volume III
Ref: ESVOL3
UK £35.00
USA \$60.00
ROW £40.00

VOLUME COMPLETE

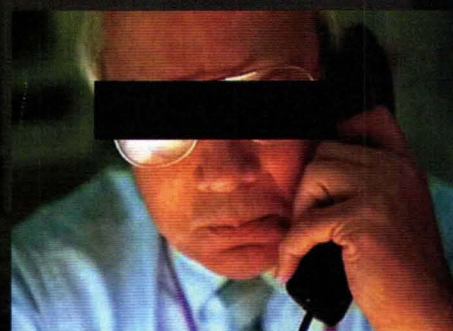
Volume IV
Ref: ESVOL4
UK £35.00
USA \$60.00
ROW £40.00

RB VALUE

WITH A FREE BINDER AND A
COPYRIGHT FREE EYE SPY INTEL
PRINTS. PRICE INCLUDES
COSTS TO ALL COUNTRIES!

VOLUME COMPLETE

Volume V
Ref: ESVOL5
UK £35.00
USA \$60.00
ROW £40.00



COMPLETE YOUR EYE SPY COLLECTION



Volume Two (eight issues)
numbers 9-16

Volume Three (eight issues)
numbers 17-24

Volume Four (eight issues)
numbers 25-32

Volume Five (eight issues)
numbers 33-40

AND FIFTH
D'S LEADING
MAGAZINE

THE
SURVEILLANCE
TRAINING
SPECIALISTS



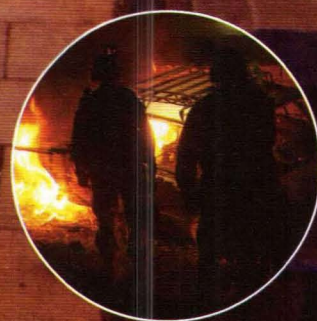
ISS TRAINING LIMITED

Established in 1990, ISS Training Ltd has been conducting surveillance training since 1996. The company is well respected within the security industry as surveillance providers. We currently provide training for:

- UK ENFORCEMENT AGENCIES • PRIVATE INVESTIGATORS
- CLOSE PROTECTION OFFICERS • ALLIED MILITARY UNITS
- SECURITY CONSULTANTS • CORPORATE SECURITY TEAMS

Training Courses

Electronic Surveillance	One Day
Foot and Mobile Surveillance	Four Days
Advanced Foot and Mobile	Five Days
Counter Surveillance	Three Days
Anti-Surveillance	One Day
Professional Witness	Two Days
Hostile Area Surveillance	Four Weeks



www.intelsecurity.co.uk



ISS Training Ltd are currently working with qualification provider Edexcel in order to certify their 40 hour Basic Foot & Mobile Surveillance Course. This qualification is expected to be a BTEC Advanced Award Level 3 and available in early 2007



ISS Training Ltd, Riverside Cottages, Nidd Walk, Pateley Bridge, Harrogate,
North Yorkshire, HG3 5NA Tel: 01423 712265 info@intelsecurity.co.uk

On 13 April 1942, U-85 had sunk the Swedish freighter *Christina Knudsen* off the coast of New Jersey and by that evening was lying on the surface in shallow water off Bodie Island north of Cape Hatteras. Shortly after midnight the destroyer USS *Roper* under the command of Lieutenant Commander Hamilton W. Howe picked up U-85 on her radar and gave chase. The U-boat was unable to outrun the destroyer and, with insufficient water under her keel to escape destruction by diving, her commander gave the order to scuttle and abandon the vessel. *Roper's* reaction was to rake U-85 with machine-gun fire killing many of the crew who were jumping into the sea. Those who survived the gunfire died soon afterwards when the destroyer churned through them while they were still struggling in the water and in an incomprehensible act of (literally) overkill dropped eleven depth charges on the already doomed U-boat. Humanity aside, apparently no consideration was given by *Roper's* commander to the potential

At the time of the sinking US Navy divers were unable to recover anything of cryptologic significance, despite attempts to do so. Citing contemporary reports, the U-85 was “...lying nearly flat on her starboard side...” and suggests this as the reason for the failure of navy divers to gain entry to the boat despite “...about one hundred descents to the wreck.” Any consideration of raising U-85 to the surface by pneumatic means was soon abandoned owing to the considerable damage to the boat’s ballast tanks caused by *Roper’s* depth charges.

THE ENIGMAS

AND OTHER RECOVERED ARTEFACTS - OF U-85

RECOVERY OF ENIGMA WHEELS

Whereas the German army (*Heer*) and air force (*Luftwaffe*) had a total of five wired wheels from which to select the three moveable wheels for daily use in their Enigmas, the navy (*Kriegsmarine*) had a total of eight wheels from which to make this selection. Since 1 February 1942 the German submarine fleet in the North Atlantic had been using an updated version of Enigma, designated *Schlüssel M* by the *Kriegsmarine*, which was equipped with an additional, non-moving fourth wheel variously called *Zusatzwalze* (additional wheel) or *Griechenwalze* (Greek wheel): this latter cognomen arising from the naming of the two variants of that wheel, 'Beta', and 'Gamma'. Each was paired with a 'thin' *Umkehrwalze* (reflector wheel), designated B and C respectively. Each combination then formed a variable reflector that could be set in any one of twenty-six positions as part of the internal machine settings. A null position was provided: when set to position 'A' the combination 'Beta/B' had the same wiring as the old 'thick' reflector B so enabling a four-wheel Enigma to communicate with the earlier three-wheel variant. The combination of 'Gamma/C' behaved in similar fashion. The Greek wheels were of an entirely different form from that of the regular Enigma wheels and thus not interchangeable with them.

In August of 1997, amateur diver Roy E. Parker, during his first exploration of U-85, recovered two oak boxes containing the spare wheels for two different Enigmas (Fig. 1). A study of these wheels determined that U-85 had been carrying two Enigmas whose inventory numbers were M2946 and M3131. The boxes were recovered from a cabinet on the bulkhead adjacent to the captain's quarters. Each contained only the normal Enigma wheels used

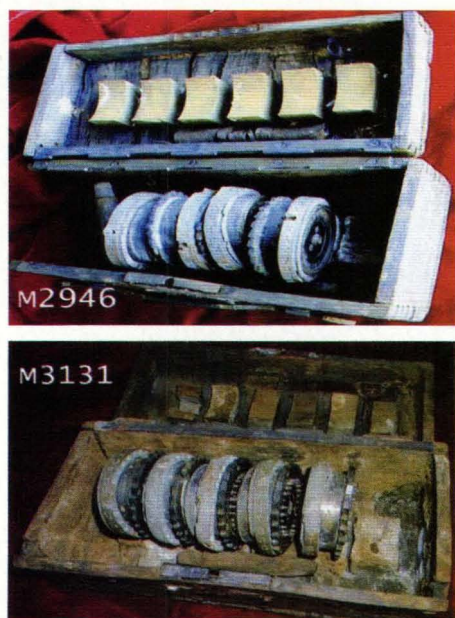


Figure 1



The typewriter that was attached to M2946 as a printing device. A fragment of the connecting cable is visible at lower left

in both the M4 and its predecessor the M3. No Greek wheels were recovered then, but the serial numbers suggested that the Enigmas to which these wheels belonged were of the newly introduced variant, M4. Details of one of the wheels from M3131 can be seen in Fig. 2 where the identification marks are clearly visible.

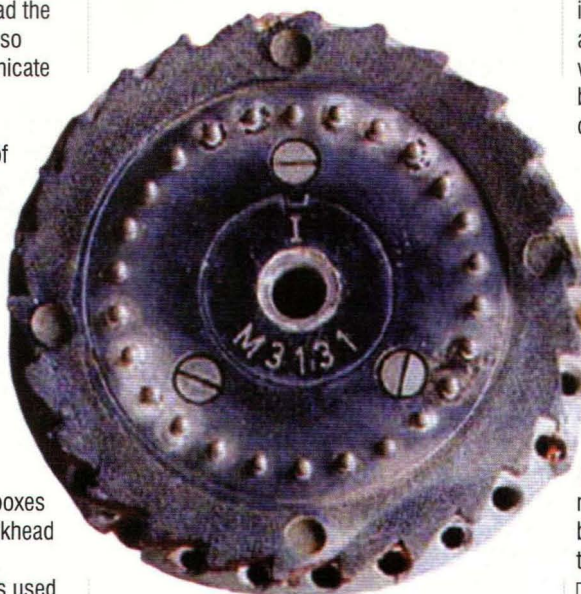


Figure 2

The recovered wheels were:

Serial Number	Wheels recovered
M2946	II, III, VI, VII
M3131	I, III, IV, VI, VIII

RECOVERY OF THE ENIGMAS

In June 2001 three divers descended upon U-85. Jim Bunch and brothers Rich and Roger Hunting had each made numerous expeditions to the site and to a number of other wrecks in the area but this time they intended to clear out 60 years of accumulated silt and debris that had hitherto prevented access to the all-important radio and sound (sonar) rooms. Over a period of approximately two weeks, using a purpose-built dredging device, they gained access to these two areas. Their task was rendered more difficult by the fact that U-85 has a list of 30-40 degrees

to starboard. The first area to be cleared sufficiently was the sound room. This surrendered a large brass compass, a wooden box containing phonograph records and, of more significant cryptologic interest, a codebook and, on a later dive, a pad of message log sheets.

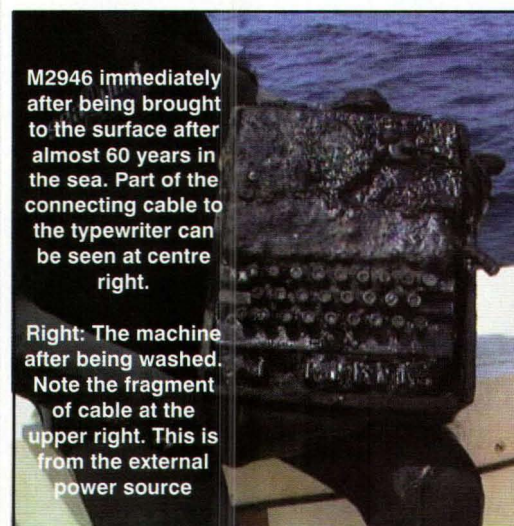
By 3 July 2001 the divers had cleared the radio room to the point that it could be entered safely and found Enigma M2946 lying on the deck in the center of the area. Nearby they found an electric typewriter that on later examination proved to have been attached to the Enigma to print the output. This was preferable to the more usual copying by hand from the Enigma's lamp panel and was of particular convenience when considering both the confined space of the U-boat and the limitations on available manpower.

Two days later the wooden lid of M2946 was found and more importantly the entire wheel cage assembly of the second Enigma, M3131. Of poignant human, rather than cryptologic, interest was the discovery of two coffee cups and a *Perrier* water bottle. No human remains were recovered - the entire crew having left the boat prior to its sinking. U-85 therefore is not considered a war-grave site.

THE CODEBOOK

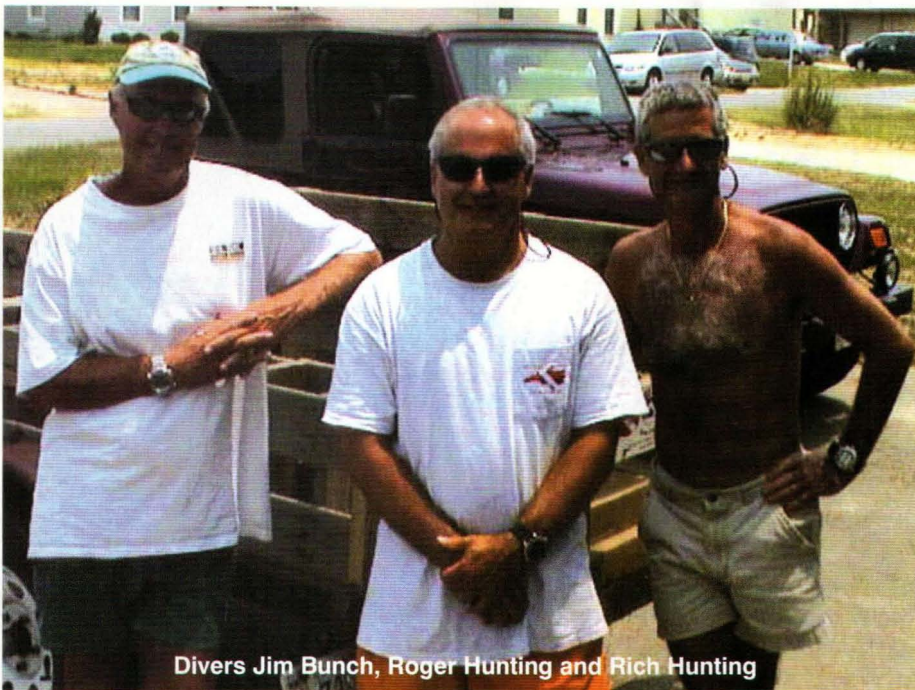
During an earlier dive, on 20 June 2001, a large block of silted material that contained a codebook was recovered from the sonar room. With enormous difficulty this was brought to the surface. Unfortunately much of the codebook was lost during this operation. A title page was recovered but regrettably it is not clear if this page refers to the entire codebook or simply to a section of something much larger in scope (though its position in the book suggests the latter). A rough translation of this page is:

**Appendix
Semaphore
Between German war- and German
merchant ships
(By order of the Naval High Command)**



M2946 immediately after being brought to the surface after almost 60 years in the sea. Part of the connecting cable to the typewriter can be seen at centre right.

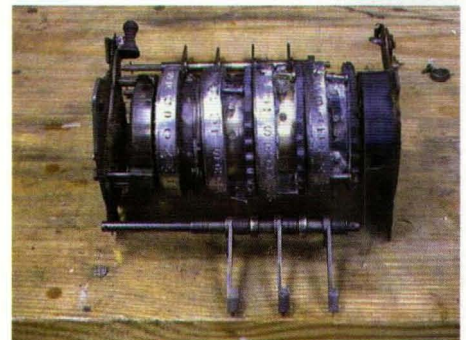
Right: The machine after being washed. Note the fragment of cable at the upper right. This is from the external power source



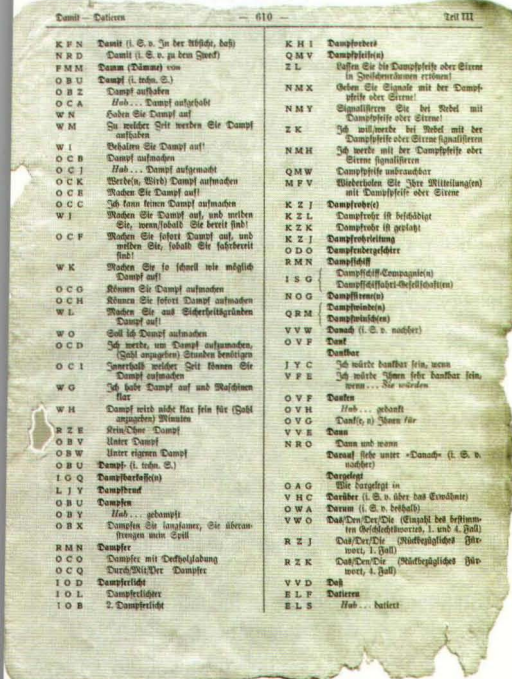
Divers Jim Bunch, Roger Hunting and Rich Hunting



M3131 recovered and restored



The wheel cage from M3131 after washing



A page of the codebook, approximately 27 x 20 centimeters, is shown above. Another title page says:



Medical section (send)

In this section meanings of flag signals with a medical content are arranged alphabetically by reference to the decoding tables. This enables signal traffic to be handled rapidly in case of sickness and accidents. These signals are no longer included in the general dictionary of the sending tables.

Recovered pages of the codebook span the range 650 to 780 and obviously represent only a fraction of the complete book. The *Winksprachverfahren* (semaphore) title page is identified as the entry to an appendix. Apparently this volume included unrecovered sections. It is interesting to speculate as to their possible content.

MESSAGE PAD

On 28 September 2001 a message pad - overall dimensions 31 x 23 centimetres - was recovered from the sonar room. Detail from the message pad is shown in Fig. 3 and begins:

Cipher-pad Secret (after being used)



Figure 3

SUMMARY

Divers have recovered artefacts from U-85 that show that at the time of its sinking the U-boat was equipped with two Enigma M4 with serial numbers M2946 and M3131. Each was provided with a full complement of eight regular wheels (I-

VIII) and at least a B/Beta *Umkehrwalze/Zusatzwalze* combination. The internal setting of each of the two Enigmas at the time of U-85's sinking was determined. M2946 was connected to an electric typewriter that acted as a printing device.

Significant fragments of a codebook were also recovered but the information gathered from this document suggests that its contents are not related to the use of Enigma. Rather, the recovered fragments refer to flag signal procedures. Several blank pages of radio message sheets, in the form of a page-numbered pad, were also recovered. A year later, on 22 August 2002, the dive team recovered the remaining parts of M3131.

© 2003. From *The Enigmas - and Other Recovered Artefacts of U-85*, by David H. Hamer. Reproduced by permission of Taylor & Francis Group, LLC., <http://www.taylorandfrancis.com>. For a full list of references contact Eye Spy.

Items recovered by the dive team are, or will be, on display at the Graveyard of the Atlantic Museum in Hatteras, North Carolina, USA:

<http://www.graveyardoftheatlantic.com/>

A gallery of the cryptologic items recovered during the dives made by Jim Bunch, Rich and Roger Hunting may be found at:

<http://home.comcast.net/~dhamer/u-85.htm>

Jim Bunch, has written about U-85 in his book *Germany's U-85: A Shadow in the Sea* published by Deep Sea Press in 2003

MAIL SURPRISE

Continued from page 45



Many companies have sophisticated postal sort machinery that detects explosives as well as chemicals

Britain's Security Service MI5 has vast experience in countering letter or parcel bombs. It's advice combined with that of the Homeland Security initiative is well worth noting.

The collective advice:

First, be suspicious if you come across mail/packages:

- It is unexpected or of unusual origin or from an unfamiliar sender
- Protruding wires
- There is any unusual smell, including but not restricted to almonds, ammonia or marzipan
- Excessive tape or string
- Oily spots, discolourations, or crystallization on the wrapper
- It seems unusually heavy for its size. Most letters weigh up to about 30g, whereas most effective letter bombs weigh 50-100g and are 5mm or more thick
- Excessive postage
- It is oddly shaped or lopsided
- Addressing mistakes and issues, including misspelled words, badly typed or written addresses, wrong titles with names, no return addresses, etc.
- It is marked 'personal', 'confidential' or 'for the strict attention of'

BOMBS
by MAIL



- The address has been printed unevenly or in an unusual way
- The writing is in an unfamiliar foreign style
- There are unusual postmarks or postage paid marks
- A Jiffy bag, or similar padded envelope, has been used
- There is a pin-sized hole in the envelope or package wrapping

Second, if you do see one or more of these tell-tale signs, persons should:

- Stop... don't handle the item
- Isolate the item immediately
- Don't open, smell, or taste it
- Activate your emergency plan and notify a supervisor

MI5 note: "Although any suspect item should be treated seriously, remember that the great majority will be false alarms and a few may be hoaxes. Try to ensure that your procedures, while effective, are not needlessly disruptive."

RECEIVING MAIL



GUIDANCE ON WHAT TO DO IF YOU SUSPECT A PACKAGE OR LETTER IS SUSPICIOUS

1. Seek advice from your local police CTSA on the threat and on defensive measures.
2. Consider processing all incoming mail and deliveries at one point only. This should ideally be off-site or in a separate building, or at least in an area that can easily be isolated and in which deliveries can be handled without taking them through other parts of the building.

FBI Advisory

If you receive a suspicious letter or package

What should you do?

1. Handle with care. Don't shake or touch.
2. Isolate and lock for authorities.
3. Don't open, handle or touch.
4. Treat it as dangerous. Don't tell.



If parcel is open and/or a threat is identified...

For a Bomb
Evacuate immediately
Call 911 (Police)
Contact local FBI

For Radiological
Limit Exposure - Don't Handle
Distance - Evacuate area
Shield yourself from object
Call 911 (Police)
Contact local FBI

For Biological or Chemical
Isolate - Don't Handle
Call 911 (Police)
Wash your hands with soap and warm water
Contact local FBI

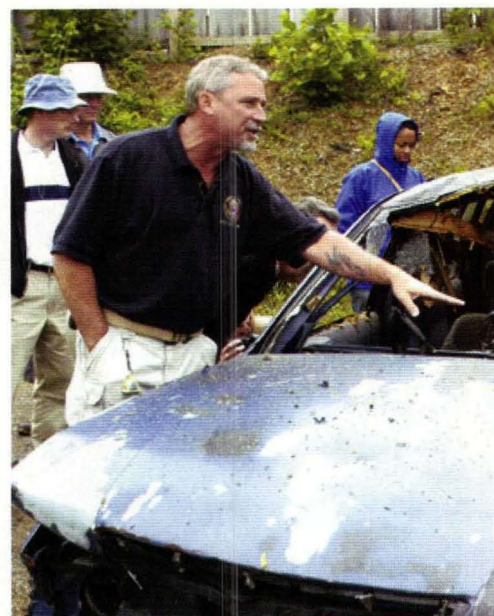


Police Department

Fire Department

Local FBI Office

(Ask for the Study Agent, Special Agent David Tschetter, or Weapons of Mass Destruction Coordinator)



3. Make sure that all staff who handle mail are briefed and trained. Include reception staff. Encourage regular correspondents to put their return address on each item.

4. Ensure that all sources of incoming mail (e.g. couriers, hand delivery) are included in your screening process.

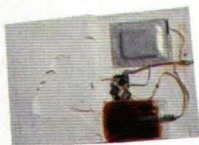
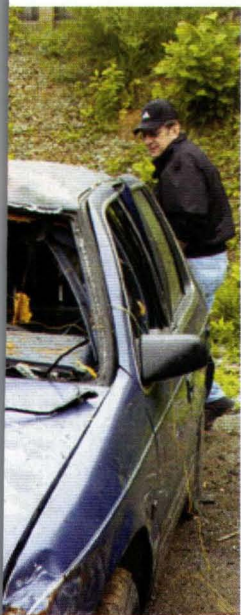
5. Ideally, post rooms should have independent air conditioning and alarm systems, as well as scanners and x-ray machines. However, while mail scanners may detect devices for spreading chemical, biological and radiological (CBR) materials (e.g. explosive devices), they will not detect the CBR materials themselves. At present, no CBR detectors are consistently capable of identifying all hazards reliably. Post rooms should also have their own washing and shower facilities, including soap and detergent.

6. Staff need to be aware of the usual pattern of deliveries and to be briefed of unusual deliveries. Train them to open post with letter openers (and with minimum movement), to keep hands away from noses and mouths and always to wash their hands afterwards. Staff should not blow into envelopes or shake them. Packages suspected of containing CBR material should ideally be placed in a double-sealed bag.

7. Consider whether staff handling post need protective equipment such as latex gloves and face masks (seek advice from a qualified health and safety expert). Keep overalls and footwear available in case staff need to remove contaminated clothing.

8. Make certain that post opening areas can be promptly evacuated. Rehearse evacuation procedures and routes, which should include washing facilities in which contaminated staff could be isolated and treated

9. Prepare signs for display to staff in the event of a suspected or actual attack.



Car bomb or machine gun fire? Neither. An instructor for Diplomatic Security's Iraq DSAC course explains damage to a car after a letter bomb is exploded on its dashboard

For employers and employees alike, countermeasures such as those identified make for essential reading and viewing.

A few minutes of your time now might just save you or a co-worker from future harm. Better yet, download or print the poster from the US Postal Service website and display it in your workplace. US readers of Eye Spy can request a free hard copy at any post office. Similarly, MI5 has some excellent advise on its website.

For more workplace security posters, see the 'Protect Your Workplace' campaign materials posted on the Department of Homeland Security website.

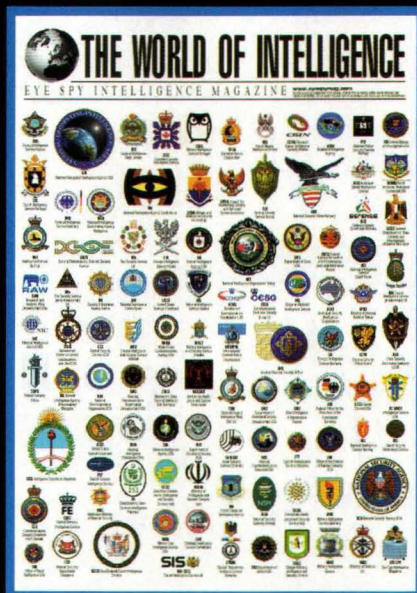


Tampering with mail will get you a new home, new friends, & a new job.

If you suspect anyone is stealing or tampering with the mail, contact your local U.S. Postal Inspectors.

EYE SPY CHRISTMAS OFFER

EYE SPY SUBSCRIBERS CAN PURCHASE A FRIEND OR FAMILY MEMBER A GIFT SUBSCRIPTION THIS CHRISTMAS AND HE/SHE WILL ALSO RECEIVE



FREE GIANT INTEL POSTER

A HIGH QUALITY FULL COLOUR GLOSS POSTER IDEAL FOR FRAMING AND DISPLAYING IN OFFICE OR HOME

Interest package:
MI6 word search
Games
Enigma
Code breaking
Intel quiz

Learn the mind of a spy

Intel files on
John Lennon
Cold War
FBI mysteries



FREE SPY PRODUCT CATALOGUE

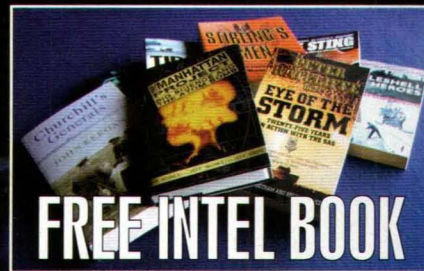
This offer is **ONLY AVAILABLE** to EYE SPY SUBSCRIBERS. Subscriptions prices are identical. All recipients will receive their first magazine plus gifts a week prior to Christmas with your name as sender. To purchase a gift subscription simply add 'Christmas' to the subscription form in this magazine or contact Eye Spy. Don't forget to include the name and address of whom the gift is intended.

Please order early as Eye Spy cannot be held responsible for delays in mailing.

Current Eye Spy subscribers can obtain their new Subscription Card by sending a SAE to Eye Spy. The card can be used to claim discounts on certain purchases



FREE NEW EYE SPY SUBSCRIPTION CARD
SAVE MONEY!



FREE INTEL BOOK

156 espionage case files from 1975-2004

Virtual tour of a nuclear submarine

Special feature on the history of intel crests and seals

13 famous detailed espionage cases

13 spy photos that changed the world

20 hi-resolution intelligence images

49 declassified intelligence articles

FREE INTELLIGENCE CD



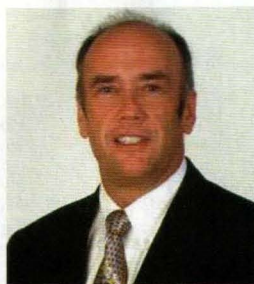
CYBERTERR

LEARNING AND UNDERSTANDING INTELLIGENCE

Cyber-terrorism or attacks on telecommunications and computer networks have been called the invisible threat to national economies and security. Day after day, digital warriors defend our information systems and infrastructure against thousands of unseen attacks by criminals and terrorists. This intelligence brief will help you fully appreciate the growing threat of cyber terrorism, the offensive capabilities of cyber terrorists, and the defensive measures that can be taken in response to such dangers. Included in this brief will be actual intelligence and scenarios that pose a significant threat to our national information and telecommunications infrastructure.

IMAGE COURTESY PACIFIC NORTHWEST NATIONAL LABORATORY/DOD

PRISM



Terrorism and information technology are related in two ways. First, the Internet has become a forum for both terrorist groups and individual terrorists to spread their messages of hate and violence.

The internet allows terrorists to communicate with one another and with sympathisers. Secondly, individuals and groups use the Internet to attack computer networks and systems via cyber-terrorism or cyber-warfare activities.

The term "cyber-terrorism" conjures up many different images. The truth is, cyber terrorism has been around longer than most people think. Cyber terrorism did not evolve after the terror attacks on 11 September 2001. According to the Federal Bureau of Investigation, cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computer programmes, networks and data, which results in violence, disruption or damage against non-combatant targets by sub-national groups or clandestine agents.



One of the first recorded cyber-terrorist attacks was in 1996. A computer hacker who was allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts Internet Service Provider (ISP) and damaged part of the ISP's record keeping system. The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "*you have yet to see true electronic terrorism... this is a promise.*"

The fear surrounding cyber-terrorism is that terrorists and other criminals could attack and penetrate critical infrastructure computer systems and endanger human lives by disrupting military networks, emergency medical services, land and air transportation systems, telecommunications and utilities. Cyber-terrorists could also cause chaos and massive disruption to business operations by attacking banking and other financial institutions that depend on computer networks for their operations. With respect to UnRestricted Warfare (see Eye Spy 43), an attack on computer systems or networks is not only one modality, but it plays a significant supporting role in many other modalities. 'Information weapons' will become the weapon of the arms race in the next decade.

In 1998, the Center for Strategic and International Studies issued a report that stated cyber-terrorists are plotting all manner of heinous attacks that, if successful, could "destabilise and eventually destroy targeted states and societies." The National Strategy to Secure Cyberspace is part of an overall effort of protection. The purpose of this strategy is to engage and empower the public and businesses to secure the portions of cyberspace that they own, operate, control, or with which they interact. However, today there are no early detection systems in place to warn of a major cyber attack.

INTELLIGENCE

More than 120 countries or foreign organisations have or are developing formal programmes to develop information weapons that can be used to attack and disrupt critical Information Systems used by the United States.

Information Weapons

There are many types of attacks that all fall under the heading of cyber-terrorism. Attack methods include:

- Computer Viruses
- Logic Bombs
- Denial of Service Attacks
- Software Vulnerability Exploitation

- 1949 - The first theories for self-replicating programmes were developed, which formed the basis of a computer virus.

- 1981 - The first three Apple viruses were seen, this is thought to be the very first virus in the world.

- 1983 - Fred Cohen, while working on his dissertation, formally defined a computer virus as "a



computer programme that can affect other computer programmes by modifying them in such a way as to include copy of itself." He also coined the term 'computer virus'.

- 1986 - Two programmers from Pakistan named Basit and Amjad replaced the executable code in the boot sector of a floppy disk with their own code designed to infect each 360kb floppy

accessed on any drive. Infected floppies had "© Brain" for a volume label.

- 1987 - The computer industry experienced the **Lehigh** virus, one of the first file viruses, which infects command.com files.

- 1988 - One of the most common viruses called **Jerusalem** was released. Activated every Friday the 13th, the virus affects both .exe and .com files and deletes any programmes run on that day.

- 1990 - Symantec **Norton AntiVirus** was launched. This is one of the first antivirus programmes developed by a large company.



- 1991 - The first widespread **polymorphic** virus was seen. These viruses make detection difficult for virus scanners by changing their appearance with each new infection.

- 1992 - 1300 viruses were in existence, an increase of 420% from December of 1990.

- 1992 - The **Dark Avenger** Mutation Engine (DAME) was created. DAME is a toolkit that turns ordinary viruses into polymorphic viruses. The Virus Creation Laboratory (VCL) is also made available. It is the first actual virus creation kit.

- 1994 - The **Good Times** email hoax tore through the computer community. The hoax warns of a malicious virus that will erase an entire hard drive just by opening an email with the subject line "Good Times." Though disproved, the hoax resurfaces every six to twelve months.

- 1995 - **Word Concept**, which became one of the most prevalent viruses in the mid-1990s was released. It is spread through Microsoft Word documents.

- 1996 - **Baza**, **Laroux** (a macro virus), and **Staog** viruses which were the first to infect Windows95 files, Excel, and Linux respectively were released.

- 1998 - The first virus to infect Java files was seen. The virus modifies CLASS files to contain a copy of itself within the middle of the file's code and to begin execution from the virus section. Many other significant viruses were released this year.

- 1998 - Two California teenage hackers infiltrated and took control of more than 500 military, government, and private sector computer systems.



- 1999 - The **Melissa** virus, W97M/Melissa, which executes a macro in a document attached to an email, which in turn forwards the document to 50 people in the user's Outlook address book infecting an estimated one million PCs was released.

- 2000 - The **Love Bug**, also known as the **ILOVEYOU** virus, which sends itself out via Outlook, much like Melissa was released. The virus comes as a VBS attachment and deletes files, including MP3, MP2, and .JPG. It also sends usernames and passwords to the virus's author.

- 2001 - The **Nimda** virus infected hundreds of thousands of computers in the world around the 11 September 2001

attacks. The virus is one of the most sophisticated to date with as many as five different methods of replicating and infecting systems.

- 2001 - The **CodeRed** attacks on vulnerable web pages and was expected to eventually reroute its attack to the White House homepage was seen. It infected approximately 359,000 hosts in the first twelve hours.



- 2002 - The author of the **Melissa** virus, David L. Smith, was sentenced



to 20 months in United States federal prison.

- 2002 - The **Klez** worm, an example of the increasing trend of worms that spread through email was first seen. Klez overwrites files with zeroes, creates hidden copies of the originals, and attempts to disable common anti-virus products.

- 2003 - The "**Slammer**" (**Sapphire**), a worm that became the fastest spreading worm to date, infecting 75,000 computers in approximately ten

minutes, doubling its numbers every 8.5 seconds in its first minute of infection was released.

- 2004 - The virus **MyDoom** or **Novarg**, spread through emails and file-sharing software faster than any previous virus or worm. MyDoom entices email recipients to open an attachment that allows hackers to access the hard drive of the infected computer.

- 2005 - The first hacking and virus attacks on cell phones and smart phones with PDAs built in was seen. The most notable was when a celebrity phone was hacked, and the contents of the contact list was taken and used.

- 2006 - Four massive virus attacks in January, including a multi-wave attack of 7 variants, started the year off badly. In February we also saw the second virus that affects Apple computers running the Mac OS X operating system, further eroding the long-held belief that Mac machines are more impervious to attacks than Microsoft's Windows-based personal computers.

COMPUTER VIRUS TIMELINE

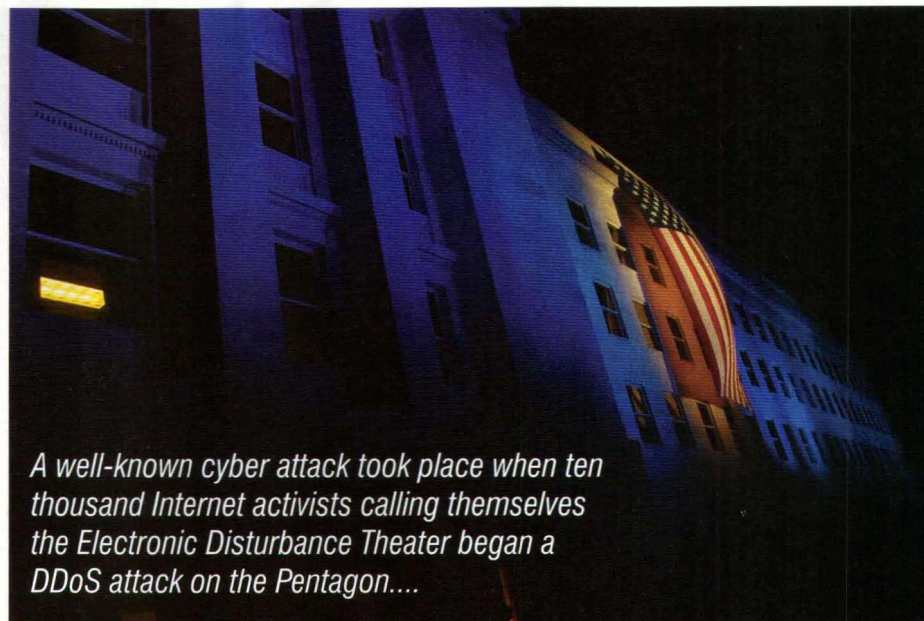
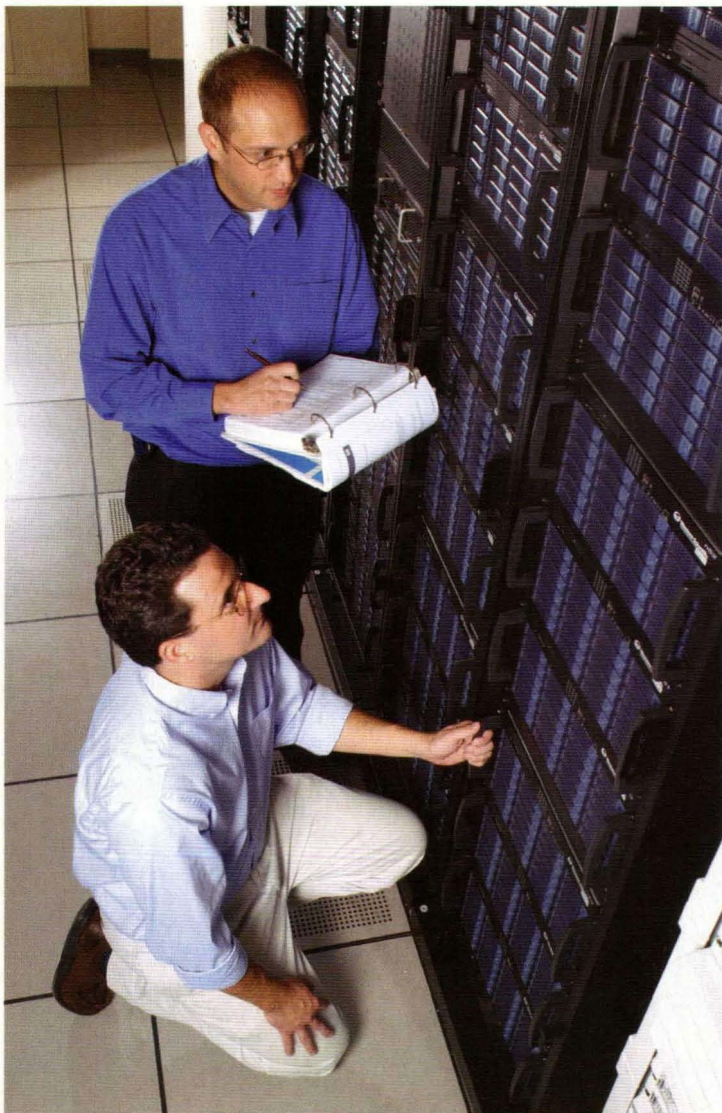
COMPUTER VIRUSES

Many people believe the first computer virus, which is considered a form of cyber-terrorism was created in 1981 and infected Apple II computers at Texas A&M. After that incident took place, an American student, Fred Cohen, was behind the first documented virus that was created as an experiment in computer security. Shortly after Cohen's work, another virus was released and another one with malicious intent was discovered. The first international virus was made in Pakistan by two programmers. They replaced the executable code in the boot sector of a floppy disk with their own code designed to infect each 360kb floppy accessed on any drive. The debate continues whether a computer virus is a cyber-terrorism attack, but most in federal law enforcement believe it is at this point in time.

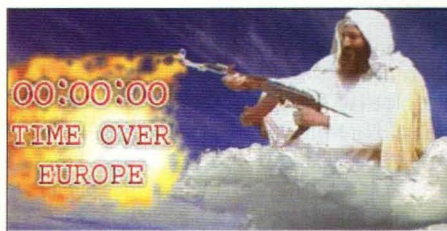
Today there are a staggering 60,000 viruses in existence, many of which have multiple mutant strains. The rate of virus creation and release has accelerated over the past few years with nearly 250 new and mutated viruses appearing each month. A computer

industry insider, who asked not to be identified, stated: "We are losing the war against computer viruses."

Viruses, as with all cyber attacks are becoming more complex, more damaging, more difficult to detect, and the frequency of viruses being released is also increasing.



A well-known cyber attack took place when ten thousand Internet activists calling themselves the Electronic Disturbance Theater began a DDoS attack on the Pentagon....



Al-Qaida has many computer experts within its ranks or sympathetic to its cause - security services around the world are convinced the terror group will sooner or later try and cause havoc via the Internet

Logic Bombs

A logic bomb is a computer programme that lies dormant in systems for a period of time until it is triggered by an event, such as a date. Once triggered, the unauthorised act is executed and more often than not is destructive in nature. Logic bombs can also be a tactic used to establish distributed denial of service attacks for multiple computers, sometimes numbering in the tens of thousands.

Denial of Service (DoS) Attacks

A Denial of Service attack is an assault on a network that floods it with so many additional

requests or transactions that regular traffic is either slowed or completely interrupted. A Distributed Denial of Service (DDoS) attack uses multiple computers throughout the network that it has previously infected. Recently, vulnerabilities in Smart cell phones have been discovered that would allow these devices to be unwilling participants in denial of service attacks. Unlike a virus or worm, which can cause severe damage to databases, a denial of service attack interrupts network service for some period.

INTELLIGENCE

A well-known cyber attack took place when ten thousand Internet activists calling themselves the Electronic Disturbance Theater began a DDoS attack on the Pentagon, Frankfurt Stock Exchange and Mexico presidential Web servers in support of Zapatista rebels in Chiapas, Mexico.

Software Vulnerabilities

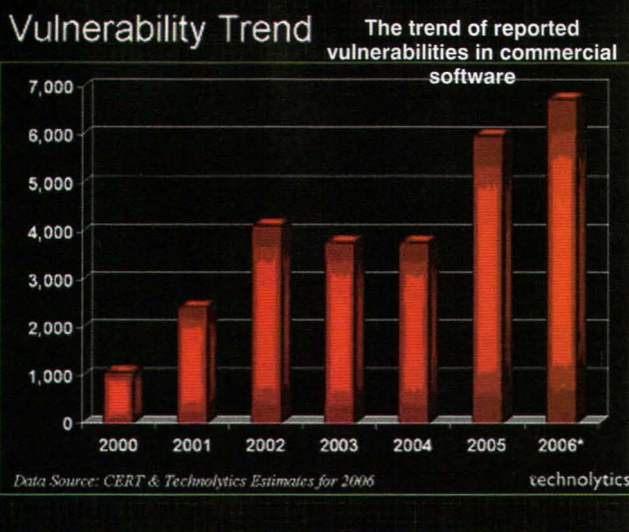
Cyber attacks have caused billions of dollars in damage and have affected the lives of millions. Recent data indicate several troubling trends. First of all the number of software vulnerabilities that can be exploited are increasing. A "software vulnerability" is ➤

defined as software which contains code that allows the software to do something it wasn't designed to do and can be used in a malicious fashion.

The increasing availability of these information weapons is partially related to certain groups whose sole purpose is to create attack kits that are sold via the internet to anyone willing to pay the price. Within the information security industry, there is wide spread belief that an organisation in South America has been created and funded with the sole purpose of developing malicious code that takes advantage of recent vulnerabilities uncovered in commercial software. The time from when a vulnerability incident is reported and announced until the first malicious code is discovered is shrinking at this time. The last few announcements of commercial software vulnerability incidents saw the exploitation code released in less than 24 hours - one taking only 17 hours. The time required for the software vendor to create a patch was 8 days.

Known Terrorist Organisations

The organisations listed in this section (see chart opposite) have been designated foreign terrorist organisations by the US State Department. (Spy-Ops expresses no opinion on the contents of this



list.) We have estimated the capabilities of each of the groups below based on open source intelligence. The capabilities can be described in four levels as follows:

Intent to Acquire - Looking to obtain cyber-terrorism capabilities.

Basic Data Weapons - Cyber weapons including viruses, trojans and basic hacking tools.

Intermediate Data Weapons - Vulnerability scanning, advanced hacking tools, denial of service tools and custom cyber attack development skills.

Advanced Data Weapons - Coordinated attack execution tools, partial packet penetration

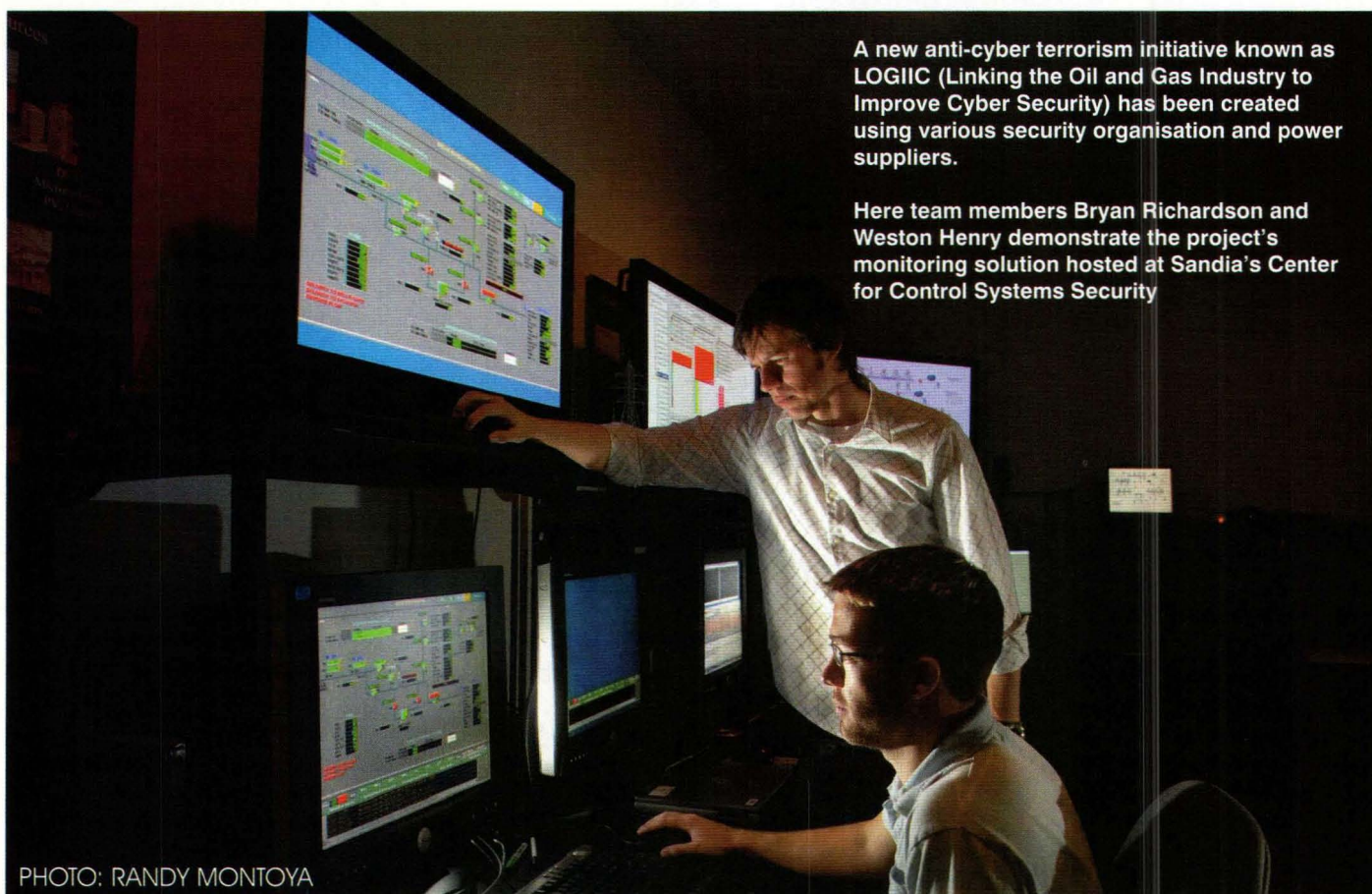
capabilities, data bombs, and alternative device hacking capabilities.

The cyber capabilities and ambition of these groups are as yet unknown. However, given the disruptive capabilities of a cyber attack, it is clear that this is a viable tool of choice for terrorists.

INTELLIGENCE

Malaysia was a favoured meeting place for the hatching of at least part of al-Qaida 9/11 terrorist plot against the United States. It has emerged as the region of choice for pro-al-Qaida cyber-terrorism. Malaysia has an advanced IT and telecommunications infrastructure. As far back as mid-2002, there was a noted increase in intrusion attacks originating from Malaysia whose country domain is .my.

The conclusion, based on this data, is that we are currently engaged in a cyber war! In the past minute there have been approximately 54,000 serious computer attacks reported to hackerwatch.org! Five percent of businesses estimate the cost of systems disruption would be over \$5 million an hour, and 60% of businesses do not know how much computer attacks cost them. Only 1% of business continuity plans address cyber attacks and only 3% address



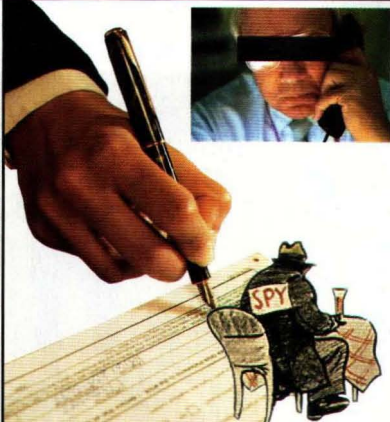
A new anti-cyber terrorism initiative known as LOGIIC (Linking the Oil and Gas Industry to Improve Cyber Security) has been created using various security organisation and power suppliers.

Here team members Bryan Richardson and Weston Henry demonstrate the project's monitoring solution hosted at Sandia's Center for Control Systems Security

PHOTO: RANDY MONTOYA

TEST YOUR SKILLS

Intel Examination



EYE SPY READERS can earn a certificate in future spy technology by completing our examination series. Send a stamped addressed envelope to Eye Spy to receive the exam papers. Complete the exams using the information contained in this feature and submit it to Eye Spy Intelligence Magazine along with a cheque or credit card information. The cost of each continuing education module is \$10 USD £5.00. Upon each successful completion of the series you will receive a colour **Certificate of Completion** that identifies the number of continuing education units for that specific programme. This professional programme has been developed through a cooperative agreement between Technolytics and Spy-Ops (USA) and Eye Spy Intelligence Magazine.

The exam paper for Tracking Terror Money, along with previous tests - Part 1 - Future Spy Technology From 'Q's' Lab (issue 34); Part 2 - DNA Technology (issue 35); Part 3 Money Laundering (issue 36); Part 4 - Digital Footprints (issue 37); Part 5 - Profiling a Terrorist (issue 38); Part 6 - UnRestricted Warfare (issue 40); Part 7 - Tracking Terror Money (issue 42) and Part 8 - Technology Warfare (issue 43) can also be downloaded at www.eyespyimag.com
For additional training briefs visit:
www.spy-ops.com

computer viruses. In a recent study conducted by the Computer Crime Research Center, 90% of respondents detected computer security breaches within the last twelve months.

The current approach for securing information assets can only be described as a reactive application of point fixes to specific and identified threats. A holistic approach is necessary to make systems markedly more secure. We have no cyber-terrorism early detection system in place. We only react after an attack is discovered, and experts will not hazard a guess as to the number of cyber-attacks that go undetected or unreported. The increased value of information weapons and tactics within the UnRestricted Warfare (URW) environment requires the development of new data weapons, alerting systems, tactical strategies, and new intelligence gathering in order to protect and defend against cyber-terrorism.

© KEVIN COLEMAN 2006

Terrorist Organization		Intent To acquire	Basic Data Weapons	Intermediate Data Weapons	Advanced Data Weapons
1	Abu Nidal Organization (ANO)	H	Y	I	P
2	Abu Sayyaf Group	M	I	P	
3	Al-Aqsa Martyrs Brigade	M	I	P	
4	Ansar al-Islam	M	I	P	
5	Armed Islamic Group (GIA)	M	Y	I	P
6	Asbat al-Ansar	M	I	I	P
7	Aum Shinrikyo	M	I	P	
8	Basque Fatherland and Liberty (ETA)	M	Y	I	
9	Communist Party of the Philippines/New People's Army (CPP/NPA)	L	I	I	
10	Continuity Irish Republican Army	L	I	I	
11	Gama'a al-Islamiyya (Islamic Group)	M	Y	I	
12	HAMAS (Islamic Resistance Movement)	H	Y	Y	P
13	Harakat ul-Mujahidin (HUM)	M	Y	I	
14	Hizballah (Party of God)	H	Y	I	
15	Islamic Jihad Group	H	Y	I	P
16	Islamic Movement of Uzbekistan (IMU)	H	Y	I	P
17	Jaiish-e-Mohammed (JEM) (Army of Mohammed)	M	Y	I	
18	Jemaah Islamiya organization (JI)	M	I	P	
19	al-Jihad (Egyptian Islamic Jihad)	M	I		
20	Kahane Chai (Kach)	L	I		
21	Kongra-Gel (KKGK, formerly Kurdistan Workers' Party, PKK, KADEK)	L	I		
22	Lashkar-e Tayyiba (LT) (Army of the Righteous)	L	I		
23	Lashkar-i Jhangvi	L	I		
24	Liberation Tigers of Tamil Eelam (LTTE)	L	I		
25	Libyan Islamic Fighting Group (LIFG)	H	Y	I	
26	Moroccan Islamic Combatant Group (GICM)	M	Y		
27	Mujahedin-e Khalq Organization (MEK)	M	Y		
28	National Liberation Army (ELN)	M	I		
29	Palestine Liberation Front (PLF)	H	Y	I	
30	Palestinian Islamic Jihad (PIJ)	H	Y	P	
31	Popular Front for the Liberation of Palestine (PFLP)	M	I	I	
32	PFLP-General Command (PFLP-GC)	L	P		
33	al-Qa'ida	H	Y	Y	P
34	Real IRA	M	Y		
35	Revolutionary Armed Forces of Colombia (FARC)	H	Y	I	P
36	Revolutionary Nuclei (formerly ELA)	L	P		
37	Revolutionary Organization 17 November	L	P		
38	Revolutionary People's Liberation Party/Front (DHKP/C)	L	I		
39	Salafist Group for Call and Combat (GSPC)	L	I		
40	Shining Path (Sendero Luminoso, SL)	L	P		
41	Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn (QJBR) (al-Qa'ida in Iraq)	H	Y	I	P
42	United Self-Defense Forces of Colombia (AUC)	H	Y	P	P

INTENT H = High M = Medium L = Low
WEAPONS Y = Currently Have I = In Process P = Planning

LOGIIC HELPS KEEP OIL, GAS CONTROL SYSTEMS SAFE

For the past 12 months, Sandia National Laboratories has served as the lead national lab in Project LOGIIC (Linking the Oil and Gas Industry to Improve Cyber Security). The project was created to keep USA oil and gas control systems safe and secure, and to help minimise the chance that a cyber attack could severely damage or cripple the oil and gas infrastructure.

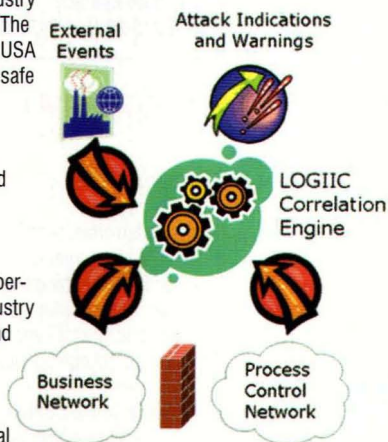
Such an attack by viruses, worms or other forms of cyber-terrorism on oil and gas industry process control networks and related systems could destabilise energy industry supply capabilities and negatively impact the national economy.

LOGIIC brought together 14 organisations to identify ways to reduce cyber vulnerabilities in process control and SCADA (Supervisory Control And Data Acquisition) systems. The goal of the project was to identify new types of security sensors for process control networks.

Sandia worked with project partners to create a simulation test bed and apply this environ-

ment to counter potential threats to the oil and gas industry using hypothetical attack scenarios. Sandia researchers created two

it's difficult to detect cyber adversaries who might be attempting to compromise critical system components."



real-time models of control systems used for refinery and pipeline operations.

"Current control system operators have limited situational awareness," said Ben Cook of Sandia. "In LOGIIC, industry leaders chose to focus the partnership team's initial work on addressing their concern that control networks aren't monitored for cyber intrusions as is routinely done on business networks. As a result,

The monitoring system developed in LOGIIC is based on the very latest commercial enterprise detection and correlation technologies adapted to monitor control networks, providing asset owners with dramatically improved situational awareness," Cook said.

To test LOGIIC's monitoring capabilities, Sandia researchers came up with five vulnerability scenarios based on cyber compromises commonly used in the hacker community. Two scenarios were extensively tested to illustrate the effectiveness of the LOGIIC monitoring solution. Ray Parks, who led the development of the scenarios, used his background as a member of Sandia's cyber red team, which has performed numerous vulnerability assessments of oil and gas and other critical infrastructure facilities.

A field test of the LOGIIC solution may begin later this year. The LOGIIC website is at www.logiic.org.

EYE SPY

UNDERCOVER BOOK RELEASES

All Eye Spy book prices
include postage and
packing - worldwide

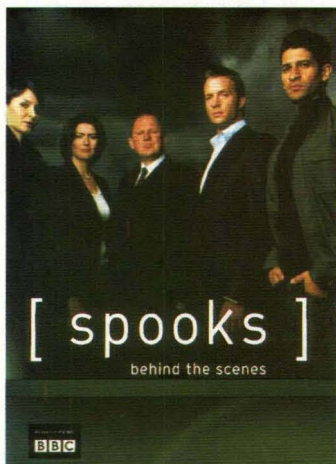
SPOOKS:

Behind the Scenes
Orion Books
ISBN: 0-75287-610-4

This extremely well-produced, near-full colour book takes the reader behind the scenes of the popular BBC fiction series about MI5.

Though the characters of *Spooks* may be a little "out of keeping" with those who actually work for MI5, the plots are carefully thought-out and many are based on real or conceivable events. The book provides a revealing insight into how the show is put together: the enormous amount of research that goes into writing the plots, the characters and how the producers try to reflect the shadowy world occupied by MI5 and its 'friends' across the River Thames - MI6. Their adversaries are also featured - from al-Qaida to Russian spies.

Series three and four are being shown in the USA, though it is called 'M-15' across the 'pond'. The book has been published to coincide with the BBC's fifth series airing in the UK right now and regularly



attracts 7 million viewers. Thirty-six episodes have been produced thus far, and the background to each and everyone is featured in *Spooks*. Of equal relevance, the unnamed authors have also chosen to incorporate dozens of sidebars - real events, spycraft, 'spy-talk' etc. It's a terrific book that provides a colourful, if inaccurate insight into MI5. The Security Service has admitted - MI5 is not nine to five - as the series always contends!

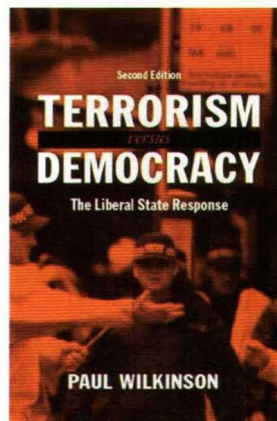
A great book for Christmas. Hardback 192pp

Available from Eye Spy
Ref: ES1186 UK £19.99 USA \$45.00

TERRORISM VERSUS DEMOCRACY
Paul Wilkinson
Routledge
ISBN: 0415384788

"No one understands terrorism better than Paul Wilkinson. If policy makers read this book they will understand the problems better. If terrorists read it they will understand themselves a lot better." - Michael Clarke, King's College London.

This acclaimed study examines both the new terror networks and those that have been around for decades. This new edition brings it up to date with the dramatic opening of the twenty first century, with new chapters on the 9/11 attacks, the growth of international terrorism, the al-Qaida network and the 'War on Terror'. This text provides us with some much needed criteria for distinguishing between terrorists and freedom fighters, and an explanation of the uses of terrorism as a political, social, religious and criminal weapon. Wilkinson also links the use of terrorism to a wider repertoire of struggle. He proposes a variety of possible counter-measures and valuable principles to



carefully distil from the recent past to help design a response that is compatible with democratic principles, the rule of law and respect for human rights. This book is essential reading for undergraduate and postgraduate students of terrorism studies, political science and international relations, as well as for policymakers and journalists.

Think you are safe by ignoring al-Qaida? Think again.

Softback 272pp

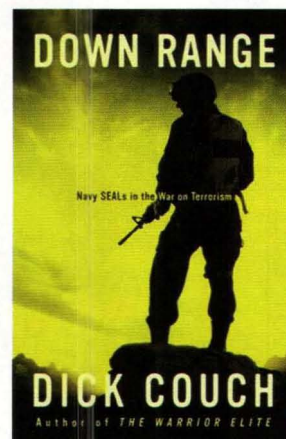
Available from Eye Spy
Ref: ES1187 UK £21.00 USA \$46.00

DOWN RANGE:

Navy Seals in the War on Terrorism
Richard Danzig (Foreword), Dick Couch
Crown Publishers
ISBN: 1400081009

Dick Couch was a SEAL member operating in Vietnam who has remained current with the current SEAL programme. He has written many books about special forces training and some of those featured in this book were men he followed through their training.

Publishers should send review copies or advisory notices to our UK or New York address featured on page 83



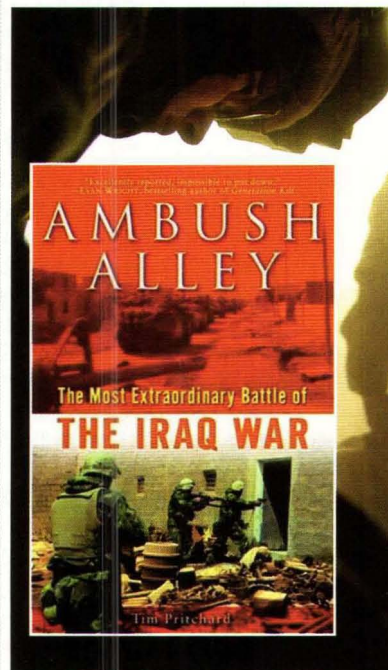
There are comparisons to the Vietnam experience, but this book illustrates just what these extraordinary men are doing and where they are operating in the continuing war on terror. A truly valuable insight by a respected insider. If you are interested in SEAL deployments, you will not want to miss this. Hardback 255pp

Available from Eye Spy
Ref: ES1188 UK £18.99 USA \$28.00

AMBUSH ALLEY:

The Most Extraordinary Battle of the Iraq War
Tim Pritchard
Presidio Press
ISBN: 0891418806

Pritchard does very well at turning a complex sequence of events into a well rounded, flowing narrative. It is the story of the US Marines attempt to secure two bridges in Nasiriyah, Iraq, in order to facilitate the progress of the main force during the 2003 invasion. They were expecting a simple, straightforward mission, but it soon turned into a nightmare of epic proportions.



What should have been an easy race to two vital bridges resulted in the main thrust being bogged down in close quarter fighting - literally in the case of the Abrams tanks, which sank into an area of sewerage. Communication was lost and forced a split in an urban area, their training took over and the troops functioned independently. The opposition was fierce, yet these troops held their ground and won. Their casualties were the highest of any single day in the conflict. The writing is focused and leaves the reader with a good overview of events. The story is related in a series of interviews with the participants which are then assembled into this gripping account of chaotic urban warfare. Highly recommended. Hardback

Available from Eye Spy
Ref: ES1189 UK £20.00 USA \$30.00

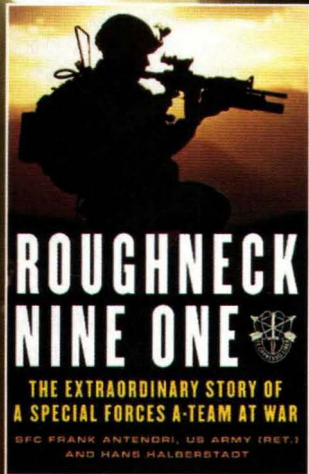
ROUGHNECK NINE-ONE:

The Extraordinary Story of a Special Forces A-Team at War
Frank Antenori & Hans Halberstadt
St. Martin's Press
ISBN: 0312353324

The story surrounding an incident early in the 2003 invasion of Iraq in which a BBC News crew and several Kurdish fighters were killed and injured. Film footage was recorded for all to see, and it wasn't too long before Coalition forces knew they had made a grave mistake.

A misdirected bomb dropped from a Navy F14 landed in the middle of newsmen and Kurdish fighters. The event was covered intensively by the world's media at the time and reports of the incident varied. Was the reporting accurate? The book gives much needed enlightenment into the seemingly complex world of US Special Forces and amply demonstrates the magnificent quality of the men involved. Hardback 265pp

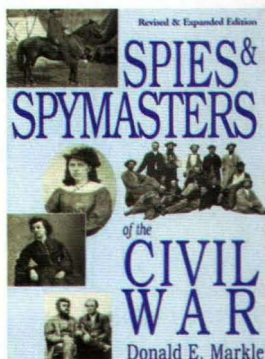
Available from Eye Spy
Ref: ES1190 UK £18.00 USA \$29.00



SPIES AND SPYMASTERS OF THE CIVIL WAR

Revised & Expanded Edition
Donald E. Markle
Hippocrene Books
ISBN 0-7818-1037-X

This book covers the entire history of American Civil War espionage for both the Union and Confederate armies. This revised edition includes new photographs and drawings and new chapters including 'After Life' - the stories of what happened to many notorious spymasters after the war, and 'Amateur Hour' - new information about the extensive intelligence gathering done by the civilian



population. The expanded edition's new chapter, 'How Far We Have Come', presents the remarkable development of American political and military intelligence from its origins in the Civil War to the present day.

The activities and tactics of hundreds of spies are described, including in-depth descriptions of spy-masters like Allan Pinkerton, Lafayette Baker, and Generals Dodge, Sharpe, and Garfield. With its appendix of all known Civil War spies -

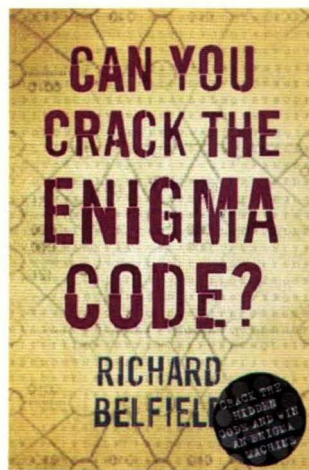
432 in all, a comprehensive bibliography of books written by Civil War spies, and a glossary of Civil War spy terms, this book is the ultimate guide to understanding Civil War espionage, and the foundation it built for modern-day military intelligence.

Now expanded with a chapter on American espionage after the Civil War!

Available from Eye Spy
Ref: ES1191 UK £16.00 USA \$14.95

CAN YOU CRACK THE ENIGMA CODE?

Richard Belfield
Orion
ISBN: 0752875264



From the earliest days of mankind, people have sought to pass on secret messages via code so that only those who are supposed to understand the message can receive it. For almost as long, cryptographers have tried to break the codes. Most famous of all were those at Bletchley Park who managed to break the Nazis 'unbreakable' Enigma.

Now, in this fascinating and intriguing book, Richard Belfield looks at some of the most difficult codes in history that have withstood years of investigation and shows the reader how they too can learn to solve or create almost any code. Sometimes, as with the notorious Zodiac Killer or the Voynich Manuscript, the codes remain unsolved, or as with Kryptos in the CIA's headquarters only 90 per cent has been decoded. Belfield explains what the current theories are

and provides avenues for further exploration.

In the final element of the book, working with a team of top cryptographers from the Royal Holloway, the author sets his own code, based on the techniques that have been revealed throughout the book. Sure to intrigue all lovers of puzzles and codes, the winning person who deciphers the code will receive an original, German World War Two Enigma machine, worth over £20,000. The publisher declares: "Can You Crack The Enigma Code? Unravel the secret code in this book, based on the techniques revealed throughout, and win an original, World War Two Enigma machine." Hardback: 336pp

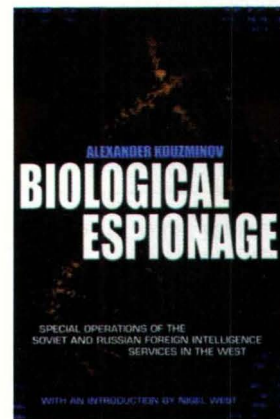
Available from Eye Spy
Ref: ES1192 UK £21.50 USA \$45.00

BIOLOGICAL ESPIONAGE:

Special Operations of the Soviet and Russian Foreign Intelligence Services in the West
Alexander Kouzminov
Greenhill Books
ISBN: 1853676462

In the wake of 9/11 the threat of biological terrorism and sabotage has been thrust to the forefront of public consciousness. However, this is far from being a new phenomenon. From World War II onwards, the Cold War powers devoted considerable resources to developing what became known in the military as 'bugs and gas'.

This groundbreaking study lifts the lid on the top-secret Department 12 of Directorate S (Special Operations) - the elite inner core of the KGB First Chief



Directorate and its successor, the Russian Foreign Intelligence Service.

During the 1980s and early 1990s the department encouraged biological espionage, the planning and preparation of biological terrorism and acts of sabotage. Their work was carried out primarily through 'Illegals' - intelligence operatives who were secretly deployed to the West and covertly operated there, masquerading as citizens of Western countries under assumed names and cover stories. One of its top operatives, Alexander Kouzminov, has decided to break his silence and reveal in depth for the first time the department's tasks, plans and tactics. More disturbingly, he explores what others in the West and the developing world are and could be capable of. In this remarkable book we learn the secrets of the USSR's elite intelligence operatives - secrets which could prove vital in maintaining international security in today's uncertain political climate. Paperback: 192pp

Available from Eye Spy
Ref: ES1193 UK £17.00 USA \$32.00

METHODS OF DISGUISE

Revised and Expanded

John Sample

ISBN: 1893626423

John Sample's creative *Methods of Disguise* is an easy-to-follow guide which includes over 130 detailed illustrations, as well as sources for makeup, uniforms, shoe lifts, badges and ID cards, contact lenses, prostheses, skin tanning preparations, fake tattoos, transvestite supplies, voice changing devices, wigs and hairpieces, and much more.

Whether you are an actor, an under-cover cop, a gambler, a practical joker, or a host for a costume party, this book will show you how to change

yourself so completely that even old friends won't recognise you! Some interesting tips - Eye Spy. Softback 258pp



Second Edition
John Sample

Available from Eye Spy

Ref: ES1194 UK £19.99 USA \$17.95

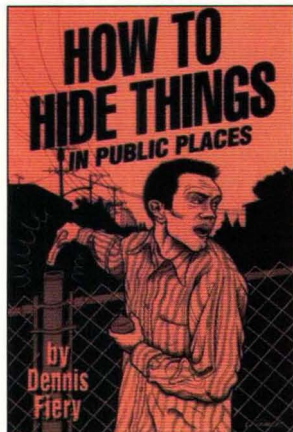
HOW TO HIDE THINGS IN PUBLIC PLACES

Dennis Fiery

ISBN: 1893626466

Did you ever want to hide something from prying eyes, yet were afraid to do so in your home? Now you can secret your valuables away from home, by following Dennis Fiery's eye-opening instructions. The world around us is filled with cubbyholes and niches that can be safely employed... and this book identifies them.

Illustrated with numerous photographs, and including an index of hiding places, appendices of Simplex lock combinations and appropriate vendors, and a bibliography, this is the most compre-



BODYGUARD

MANUAL

REVISED EDITION

LEROY THOMPSON

BODYGUARD MANUAL

Revised Edition

Leroy Thompson

ISBN: 1853676624

Provides a fascinating insight into this most dangerous of professions and draws on the experience of the world's finest operatives.

Although military operations against terrorist forces often grab the headlines, the men and women who protect government, military and business leaders from assassination or kidnapping are also in the frontline in the war against extortion and terrorism. Ready and prepared to place their body between their employer and a bullet, the bodyguard must be able to blend into the

background around their charge, yet be ready to act instantly to counter an attack. Based on techniques of the US Secret Service, US State Department Security, the Special Air Service, the Royal Corps of Military Police, the Metropolitan Police, the KGB and its successor the FSB, France's GSPR, and other protective units around the world, the *Bodyguard Manual* details the steps a protective team takes to prevent attack as well as the tactics which are employed when it is necessary to counter an attack. From providing security aboard Concorde, the Orient Express or the Queen Elizabeth II, to protecting a high-ranking officer in combat, the *Bodyguard Manual* allows the reader to 'stand post' with the professional bodyguard.

Eye Spy readers have requested a good replacement for Peter Consterdine's *Modern Bodyguard* which is at present unavailable. This offering from Thompson is a useful option.

This revised edition brings the book completely up to date, covering

developments in the field since first publication. Fully illustrated with diagrams and photographs. Softback 192pp

Available from Eye Spy

Ref: ES1198 UK £16.99 USA \$27.50

HAVE PASSPORT, WILL TRAVEL:

Field Notes for the Modern Bodyguard

Paul G. Markel

Publisher: AuthorHouse

ISBN: 1420817833

You don't have to be a professional bodyguard to appreciate *Have Passport, Will Travel*. Any person that is concerned with their own security and how to keep their loved ones safe can learn valuable lessons from the text. Chapters dealing with travel safety, understanding the criminal mind, and how to choose the correct weapons and ammunition for self-

defence will appeal to all security conscious individuals.

The aspiring professionals will value the sections dealing with advanced work,



hensive and informative book ever written about public hiding spots.

The author contends that by following the text of this useful manual, it "eliminates the risks involved with hiding your possessions at home." Softback 216pp

Available from Eye Spy

Ref: ES1195 UK £18.00 USA \$18.00

BIG BOOK OF SECRET HIDING PLACES

Jack Luger

ISBN: 1893626091

The biggest and best book on concealment of physical objects ever printed. This huge book tells how searchers find hidden contraband and how to hide things so it can't be found. Topics

covered include identifying hiding places in the home, on your person and in automobiles, descriptions of the different types of searchers you may encounter, and the intensity of the searches they may conduct, as well as the tools and techniques searchers use, including mirrors, metal detectors, vapour detector, dogs, and more. And what items might you need to hide? A partial list might include things that must remain secret, or items that can be easily hidden and easily stolen. Softback 124pp

Available from Eye Spy

Ref: ES1196 UK £20.00 USA \$20.00

SURVIVAL DRIVING:

Staying Alive on the World's Most Dangerous Roads

Robert H. Deatherage Jr.

ISBN: 0873646339

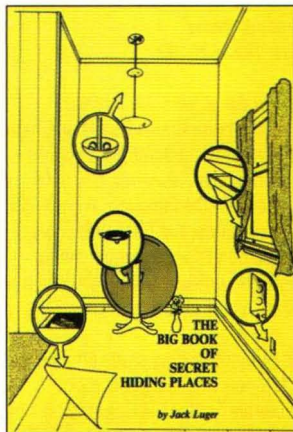
In any high-risk area, you are most vulnerable when in a vehicle en-route to your home, office or other regular destination. No one knows this better than Robert H. Deatherage Jr., who has more than 20 years experience in antiterrorism in both the military and private sectors. In *Survival Driving*, Deatherage takes the antiterrorist driving lessons he learned from today's war zones and shows you how to adapt them to your situation, whether you are in Baghdad, Beirut, Bogotá or Brooklyn.

Using straightforward rules, security checklists, photographs and drawings,



he teaches you how to prepare a route analysis, including marking maps and identifying choke points and safe havens; recognise likely attack sites for IEDs, ramblings, drive-by shootings and overrun attacks; reinforce and maintain your vehicles to withstand attack by selecting the proper armouring, engine, tires, alarms, windows, locks and more; spot surveillance whether it's fixed or mobile; master the driving basics of steering, braking and accelerating, as well as advanced evasive manoeuvres such as forward and reverse 180-degree turns and barricade breaching; and scrutinize military or police personnel at roadblocks or accident scenes to tell whether they are real or fake.

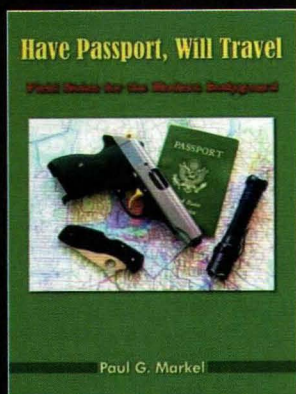
In the final chapter, Deatherage evaluates actual vehicle attacks and explains how the simple lessons taught in this book might have enabled the victims to avoid the attacks or use evasive manoeuvres to outrun their attackers. Whether you are an enlisted man or reservist about to be deployed, a security contractor or



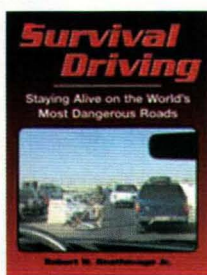
foreign travel, communications equipment, and the numerous checklists found inside. Jack McGeorge a close protection officer and former member of the US Secret Service said: "Our profession has long needed an alternative textbook - *Have Passport, Will Travel* - should be required reading for those new to the business and will be invaluable to those of us who have been around a while.

This book has been around for about 18 months, but it hardly received the publicity it deserved. Softback 116pp

Available from Eye Spy
Ref: ES1199 UK £15.00 USA \$14.00



businessman stationed overseas or just a daily commuter who travels on some dangerous roads, you owe it to yourself to take this crash course in survival driving.

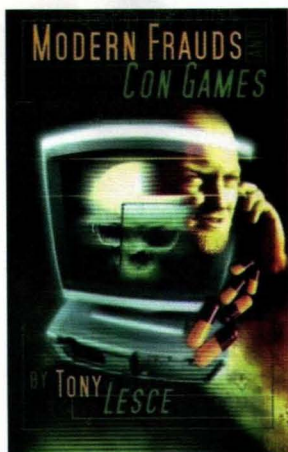


Robert Deatherage served in the US Army Special Forces in some of the world's most dangerous areas, where he was responsible for the security of GIs and their equipment. Most recently, he was the security manager for an international contractor in various regions of Iraq. He has attended the most prestigious driving courses in the world, including those conducted for Special Forces, FBI and United Nations personnel. Softback 160pp

Available from Eye Spy
Ref: ES1197 UK £24.00 USA \$25.00

MODERN FRAUDS AND CON GAMES
Tony Lesce
ISBN: 155950224X

Fraud is the fastest growing industry in the world, which is why it's become a global trillion-dollar problem. The main reason is that it's low-risk compared to other crimes. Overall, the apprehension rate is about three percent and the



conviction rate about one percent. This volume describes dozens of frauds, many of which are not even illegal but do involve deception for economic gain. This book will shed light on the new frauds and con games, with an extensive chapter on steps you can take to reduce your vulnerability to fraud. No book on fraud can be the final word, but this one will help you protect yourself and your family. Softback 178pp

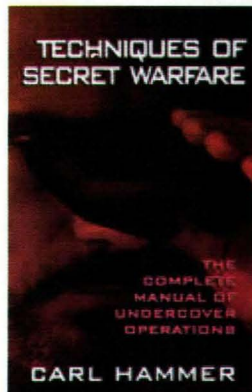
Available from Eye Spy
Ref: ES1200 UK £14.99 USA \$17.50

TECHNIQUES OF SECRET WARFARE:
The Complete Manual of Undercover Operations
Carl Hammer

Now you can study the techniques used by real professional spies and investigators. Learn how to gather any type of information you may want - or stop others from getting information on you!

Examples from real operations and case histories are included to illustrate the techniques described. This is vital information for everyone interested in intelligence-gathering or privacy. Softback 174pp

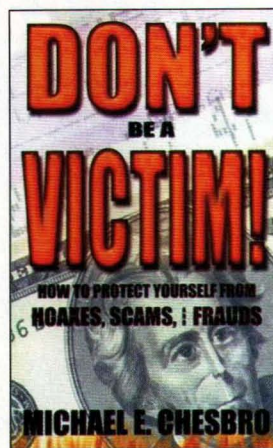
Available from Eye Spy
Ref: ES1201 UK £14.95 USA \$14.95



**All Eye Spy prices
include postage and
packing**

DON'T BE A VICTIM!
How to Protect Yourself from Hoaxes,
Scams, and Frauds
Michael Chesbro
ISBN: 1559502304

This book looks at various hoaxes, scams, and types of fraud. You will learn to recognise these crimes for what they are and look at what you can do to protect yourself from becoming a victim. It is important to remember, however, that no book can identify every possible hoax, scam or fraud, or every variation on these crimes. There will always be some new twist, some new way that criminals find to take advantage of the unsuspecting.



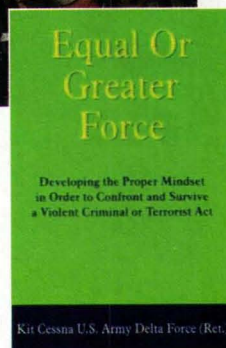
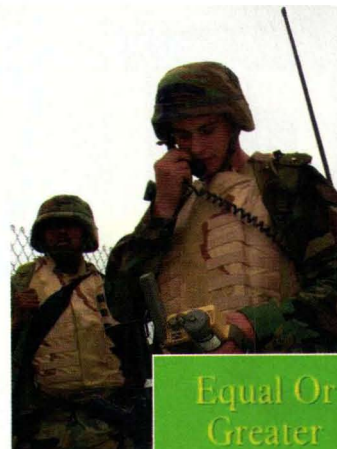
However, by recognising the most common of these crimes and the underlying principles that make them successful, this offers protection.

Fraudsters will as easily take your life savings, trick you into paying for goods you will never receive or steal your complete identity, as they would catch a bus. At the very least, this useful guide gives the reader an insight into how people fall victim to thugs and criminals. Softback 143pp

Available from Eye Spy
Ref: ES1202 UK £14.99 USA \$15.00

EQUAL OR GREATER FORCE:
A Delta Force Veteran Teaches You How
to Survive Crime, Terrorism, Natural
Disasters, and Other Calamities
Kit Cessna
ISBN: 1420809687

Kit Cessna, a combat-tested veteran of the US Army's supersecret Delta Force, knows a lot about survival. Drawing on his experience as a career soldier, a SWAT officer and a Louisiana resident who provided security during Hurricane Katrina, Cessna examines what it takes to survive today and offers a wake-up call for those citizens who expect the government, or anyone else, to take care of them in any disaster, natural or man-made. Cessna's number one rule for survival is that the party primarily responsible for your continued existence



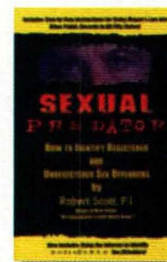
is you. This book will teach you how to develop a stay-alive attitude, make yourself mentally tough enough for any situation, control your fear during a confrontation, choose the right weapon for various situations and deal with the emotional and legal aftermath of an attack or natural disaster.

Kit Cessna served in the 1st Special Forces Operational Detachment - Delta (Delta Force), 2nd Ranger Battalion and the 1st Special Forces Group as an A-Team member. While in Delta Force, he saw combat action in the 1989 invasion of Panama. Currently, he is an instructor for the US State Department Anti-Terrorism Assistance Programme and is the lead instructor for the Southern Anti-Terrorist Training Academy in Louisiana. Softback 146pp

Available from Eye Spy
Ref: ES1203 UK £17.00 USA \$17.00

SEXUAL PREDATOR
How to Identify Registered and
Unregistered Sex Offenders
Robert Scott

Is there a sexual predator in your town? Fact: in the USA alone, more than half a million persons previously convicted of rape, molestation and other sexual assaults have been released from prison and are living in society. Here's a little-known secret: the government keeps lists of these sex offenders, and the information is available to the public for those who know where to look. Renowned private investigator Robert Scott, author of *The Investigator's Little Black Book*, unlocks the secrets to identifying registered and unregistered sexual criminals. A must for anyone who needs to check into the background of acquaintances, child care workers, employees, neighbours and others. Softback 277pp



Available from Eye Spy
Ref: ES1204 UK £15.95 USA \$14.95

EYE SPY

PRODUCT REVIEW

PowerMonkey

THE ULTIMATE EMERGENCY CHARGER



We've all been there. Away from home, nowhere near the car, on a train or coach and you haven't got the mains powered charger with you (which is fine because you don't have access to a wall socket anyway) and your cell phone or laptop computer has just run out of battery power. Or maybe your surveillance camera battery has just died and the target is getting away or your radio is out of range and you find it necessary to revert to a cell phone... but the battery has just failed. Well, there is a new product on the market which will help you avoid such situations - it's called The 'PowerMonkey'.

Small size, light weight and cleverly crafted design, plus its highly competitive cost means the device is likely to become an essential piece of kit in future months. Besides being an important addition to the surveillance industry, it will interest businessmen, regular train and aeroplane users, walkers and anyone who uses electronic equipment in open or remote environments. Parents should definitely make sure their children carry the unit when venturing out in town or to a party etc. It's easily tucked away in the pocket or handbag.

Eye Spy understands its creator was a British soldier in an operational area who found

himself with a dead cell phone - it's a situation that could have been life-threatening. For soldiers in the field, the PowerMonkey will augment essential equipment.

Eye Spy put the PowerMonkey through its paces and we believe it could revolutionise the way in which you charge your devices.

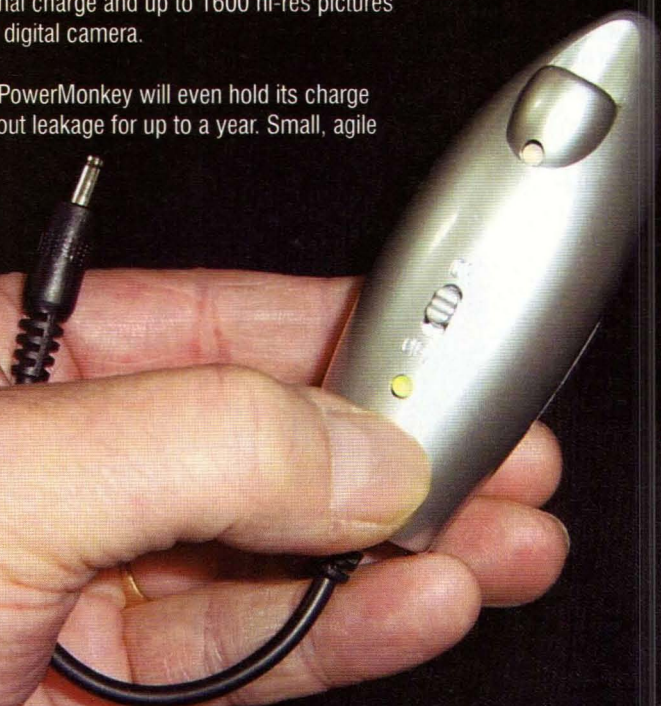
It's been likened to a portable petrol pump for your technology.

Prior to our test, we used the included mains adaptor to fully charge the PowerMonkey. It performed very well and supplied over 90 hours standby on our cell phone, nearly 22 hours on our two-way radios, 40 hours on an iPod, 6 hours on a Sony PSP, two full charges on a PDA plus it's original charge and up to 1600 hi-res pictures on a digital camera.

The PowerMonkey will even hold its charge without leakage for up to a year. Small, agile



Just some of the equipment connectors included with the kit - others are readily available





An ideal surveillance tool

and powerful, this innovative device can be left in the car, desk, briefcase, handbag etc. and will be ready to provide you with emergency power when you need it most. It's ideal for surveillance jobs where you might have several types of technology with you. People may find that using PowerMonkey eliminates the need for bulky chargers taking up lots of space or the cost of additional swap batteries. They may be correct. However, for professionals we would always advise such equipment is carried. Nevertheless, if this is not convenient simply use the PowerMonkey and its connectors (several popular units included) to charge various devices.

PowerMonkey features 2 LEDs; 1) PowerMonkey Charging: flashes red when PowerMonkey needs charging, shows red whilst charging and green when fully charged. 2) Device Charging: flashes green when discharging to device and red when low battery voltage. Importantly, the universal mains charger will work in over 150 countries and has interchangeable heads for use in the UK, USA, Australia and Europe.

The unit comes with:

- Nokia & Mini Nokia, Motorola V series, Samsung A288, Siemens C25 and Sony Ericsson wide connectors.
- 1 mini USB for Motorola Raza V series, Blackberry and Bluetooth headsets

- USB for iPod, smart phones, PDA and other devices
- Connector for Sony PSP and most digital cameras
- Black felt travel pouch

PowerMonkey worked well with numerous digital cameras, but it didn't have an adapter for older models, these, however, are available from most good electronic shops.

It's performance and adaptability make PowerMonkey an essential

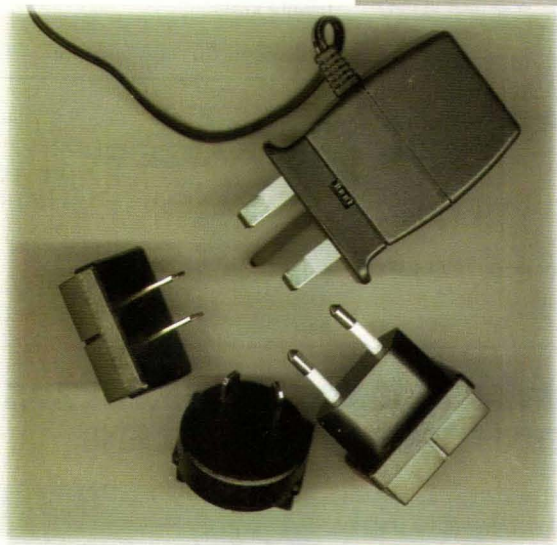
that will undoubtedly become popular with millions of people. And, there are no batteries required!

Available from Eye Spy

Order code PT-PWRMNK3

UK £35.00 USA \$70.00

ROW £40.00



PowerMonkey on charge - the kit comes with chargers for the UK, USA, Europe and Australasia

piece of equipment for the professional and public alike. For field operatives and private investigators it's worth its weight in gold, but it is definitely a product Eye Spy recommends to all families. So simple to use and with a wide variety of connectors (which can be added to) PowerMonkey is a terrific device



EYE SPY ON- LINE

CHECK OUT OUR MASSIVE NEW
RANGE OF SURVEILLANCE
PRODUCTS AT

www.eyespy.com

NEW RANGE

COMPUTER MOUSE TRANSMITTER

As soon as this computer mouse is connected to a computer it transmits sounds to a receiver for listening and recording. If you want to know what's going on in your computer room this covert device is outstanding. Requires no additional wiring.



UK £299.00 USA \$550.00 ROW: £315.00 Order code: RV-MT

MICRO GPS/GSM TRACKER



Miniature covert vehicle tracking unit, self contained, with built in long life rechargeable battery, GPS antennae and SIM card slot. Simply dial the tracker from your mobile phone and then you will instantly be sent a text message containing coordinates of its location. Simply enter these coordinates into a map and you will be shown its location down to street level. Unit measures 45 x 66 x 25mm. Weighs just 90gm.

Now with Sirf III technology enabling you to deploy the Micro Tracker inside the vehicle too.

UK £699.00 USA \$1250.00 ROW: £750.00 Order code: RV-MGPSL

Compatible European map only £50.00

WORLDWIDE OPERATIONAL GPS/GSM TRACK & LISTEN TRANSMITTER

Miniature covert vehicle tracking unit, self contained, with built in long life rechargeable battery, GPS antennae and SIM card slot. Now with a built-in sensitive microphone. Simply dial the tracker from your mobile phone and then you will be able to listen into the surrounding conversations. The Micro Tracker can be programmed to automatically send you location reports (SMS) at requested intervals. The text message (SMS) report will contain coordinates of its location, simply enter these coordinates into a map and you will be shown its location down to street level.

Now with Sirf III technology enabling you to deploy the Micro Tracker inside the vehicle too. Measures 45 x 66 x 25mm. Weighs 90gm. Optional UK or European map.



WARNING: Some of the products advertised in this magazine may be illegal to operate in your country. Please familiarise yourself with the law as it affects you.

EYE SPY'S ULTIMATE SPY PHONE INTERCEPTOR

SPYPHONE AND TEXT FORWARDING
WITH REMOTE CONTROL

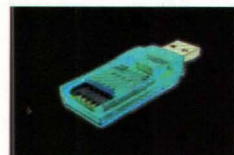
Install the intelligent software and you will be able to dial in and listen to the surrounding sounds and conversations coming from around the target phone from ANYWHERE in the world without any indication of connection. Every time the target makes or receives a text message on this phone you will instantly be sent a copy. There will not be a log and the copy will include the number of person who sent or received the text. A very powerful espionage device.

UK £850.00 USA \$1500.00
ROW: £900.00
Order code: OL-OLS



DELETED TEXT MESSAGE READER

This clever device allows you to read the deleted messages stored in a mobile telephone SIM card. Simply connect the device to your USB port on your PC/Laptop then insert the target SIM card into the reader and using the software provided you can retrieve deleted text messages. Package comes complete with software and reader. Ideal for private investigators, concerned parents or worried spouses!



UK £240.00 USA \$500.00 ROW: £250.00 Order code: RV-DTR

VOICE CHANGER PHONE



A stylish fully-working telephone with a voice changer built-in. The voice changer can be switched on and off and comes complete with eight different settings. This phone requires no external power. Also available in black.

UK £160.00 USA \$350.00 ROW: £175.00
Order code: RV-VCP

RECORD PHONE CONVERSATIONS

Record single line telephone conversations for further proof in disputes. Simply connect to any telephone socket at home or work and record two-way conversations clearly on any recorder. If you connect it to a voice activated recorder you can record automatically every time the telephone line is in use.



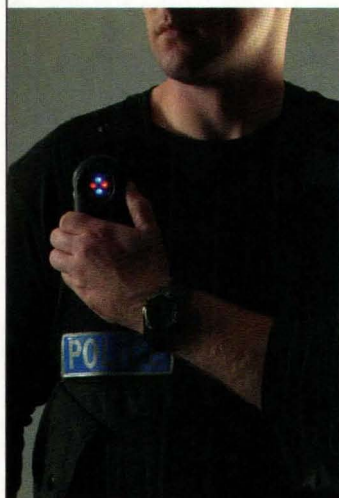
UK ONLY £35.00
Order code: RV-SLR



UK £1050.00 USA \$2000.00
ROW: £1100.00
Order code: RV-MGPSWW

NIGHTPALM PC8

Don't leave home without it!



Multi-functional torch and signalling device. A highly-rated and versatile piece of equipment - ideal for numerous tasks including emergency situations

PC8 POLICE

red/blue/white lights

PC8 OUTDOOR

red/green/white lights

For full description of functions see www.eyespy.com or send for our free equipment catalogue

Order codes:

PC8 Police or PC8 Outdoor
(please state option)

UK £40.00 USA \$85.00
ROW £45.00

PROFESSIONAL BODY WORN COVERT EARPIECE

Covert ear piece for undercover communication operations. Complete with miniature body-worn transducer and microphone for two way communication.

This system's communication is based on GSM therefore providing an unlimited communication range.



UK £850.00 USA \$1500.00
ROW: £875.00
Order code: RV-CEP

REX PLUS - ELECTRONIC RADAR WATCHDOG



UK £90.00
USA \$125.00
ROW: £100.00
Order code:
TX-EWREX

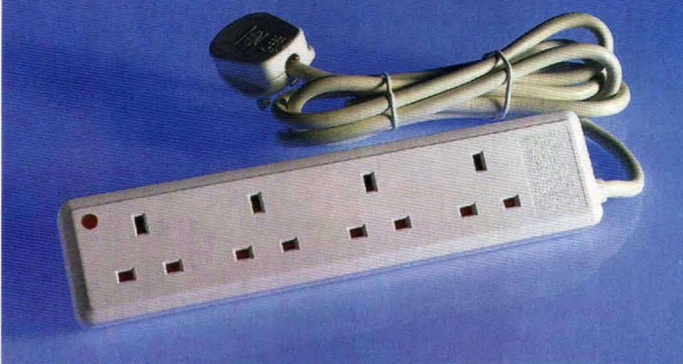
EYE SPY BEST-SELLER

This highly rated product is one of the best anti-burglar-intruder systems available today. Simply turn on (no installation required) and the realistic dog bark sound increases as its internal radar senses someone approaching the door.

Bark gets louder as person nears door. Review appeared in Eye Spy 41 and we now have dozens of satisfied customers. Protect your home, family or office with this superb security system.



ELECTRICAL EXTENSION BUG



Extension sockets can be found anywhere, but this one is slightly different. Extension socket has built-in UHF transmitter. The microphone is very sensitive and you can listen or record up to 100m range. Use with our UHF receivers.

UK ONLY £285.00 Order code: RV-EEB

PORTABLE ACRYLIC INSPECTION MIRROR

Security inspection where vision is obscured. Used by professional bomb squads, drug search, customs, airlines, security and armed forces. Very bright reflection. Shatter resistant lightweight acrylic. Don't confuse this model with cheap replicas.



15cm diameter (5.9 inches) or 23cm diameter (9.2 inches). Extending arm to 1 metre. Folds away after use

15cm model UK £235.00 USA \$400.00 ROW: £250.00
Order code: RV-AIM15

23cm model UK £275.00 USA \$499.00 ROW: £285.00
Order code: RV-AIM23

POLICE STANDARD REVERSE PEEP-HOLE VIEWER



The 'Reverse Peep-Hole Viewer' was developed with the help of the law enforcement industry to help them assess potential hazards behind doors. The unit is simple to use. The officer places it over the peephole in the door and can look into the dwelling without alerting anyone inside. They can assess any potential threats or activity before proceeding with their mission. The unit fits 99% of most common peepholes used in apartments, condominiums and houses. Reverse Peep-Hole Viewer can be used in most other countries. Made of high quality lightweight materials, its housing is a strong, lightweight composite with an all-weather coating. The lenses are high-quality precision ground glass and custom designed for Reverse Peep-Hole Viewer.

Order code: TX-RPV UK £95.00 USA \$159.50 ROW £100.00

TELEPHONE RECORDING TO PC

You can use your computer for recording telephone conversations. Store the data safely on your hard disk. Product comes with everything you need to store voice data.



UK £155.00 USA \$300.00
ROW: £165.00
Order code: RV-TCRS

BEST SELLERS

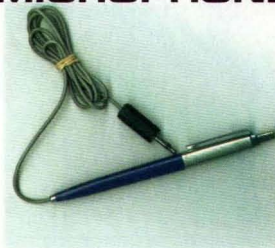
EYE SPY SEED MICROPHONE



Seed microphone so small it can be concealed anywhere - hide in a car, under door, bag, sleeve, belt etc. The length of lead is 36 inches - but we can customise this for you - £1.00 (\$1.75) for every additional 12 inches. The microphone head is just 5mm in width

Order Code: LS-SM1 UK £17.50
USA \$38.00 ROW £18.00

EYE SPY PEN MICROPHONE



Contained inside the ordinary pen is a powerful microphone. Simply plug the lead into a recorder and record any conversation without the worry of trying to hide a body-worn microphone. Can be hidden in a desk etc.

Order code: L-PN1 UK £25.00
USA \$48.00 ROW £28.00

EYE SPY DIY



Continued from page 17

for later reference or evidence in court. A toy microscope with a 10x or 20x magnification level is fine, even if the optics are made of cheap plastic. If it didn't come with a lens cap, any plastic cap that fits over the lens will suffice. Make sure the area is well lit from the sides using a desk lamp or flashlight.

You can use the same method to adapt your digital camera. Make sure the alignment is as close to parallel as possible and avoid getting ambient light between the camera and sight as it will cause the camera to open its iris darkening the images. Experiment with the camera exposures - you may need to turn off the flash and set the exposures manually and don't use the camera's zoom function.



The finished product

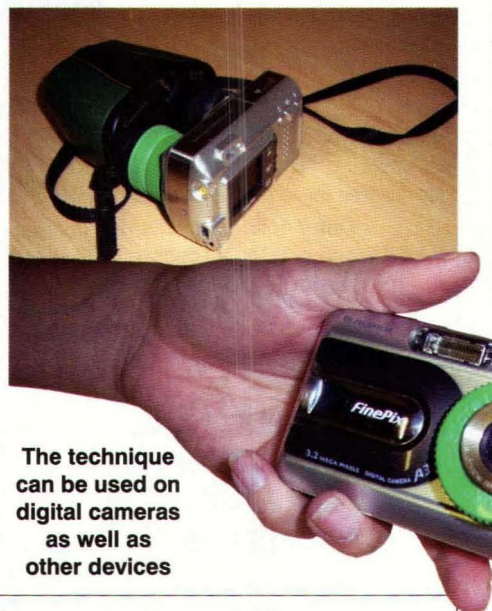


An untouched screen shot from our monitor after the camera was attached to the binoculars. The dark arch is caused by the caps

When adapting a camera to a telescope, you will roughly double the range of binoculars but the alignment is critical. If it is even slightly off you will get a picture of the inside of the telescope. You may want to fasten a tube of some sort that fits snugly over the camera lens and the telescope eyepiece. The distance between the camera lens and the eyepiece is also fairly critical, but once your tube is in place, it is easy to slide either end back and forth to find the correct position. Experiment with PVC tubes found in any hardware store plumbing section. Make sure to choose the black variety. PVC is a good choice because it is stiff, but easily filed, drilled, and even heated and melted into what ever shape you might need.

Using a base made from wood or plastic, mounted to a tripod is easy as the tripod has mounting threads. Attach the base to the tripod and put the camera/scope on the base. You should be able to see a license plate from a mile away. Remember you give up light for distance at magnified levels, so a computer programme that

alters image brightness and contrast may be necessary. A telescope with levels up to 250x works well, but at higher levels image quality becomes poor and distorted.



The technique can be used on digital cameras as well as other devices

OFFICIAL EYE SPY ORDER FORM 2006/7

ref	price	ref	price
		total £ or \$	

name _____

address _____

post/zip code _____ country _____

method of payment [A] cheque [] credit card [B] []

Cheques/Postal Orders payable to: 'EYE SPY PUBLISHING LTD'

card number _____

expiry date _____ Last 3-digits on reverse of card (security code) _____

issue number (Switch UK only) _____



UK, EUROPE AND REST OF WORLD



Eye Spy Magazine, P.O. Box 10,
Skipton, North Yorkshire, BD23 5US, England
Or Telephone: 01756 770199 (UK) standard rates



UNITED STATES OF AMERICA

Eye Spy Magazine, Empire State Building,
350 Fifth Ave, Suite 3304-22H, New York,
NY 10118-0069, United States of America
Or Telephone TOLL FREE 877 309 9243



CANADA

Eye Spy Magazine, Canadian Bureau
P.O. Box 153, Port Perry, Ontario,
Canada, L9L 1A3
Or Telephone TOLL FREE 877 309 9243

WE NOW ACCEPT ORDERS VIA PAY PAL eyespy@eyespy.com

INTERNATIONAL INTELLIGENCE MAGAZINE

UK Editorial Address: Eye Spy Publishing Ltd,
P. O. Box 10, Skipton, North Yorkshire,
BD23 5US, England
Telephone: 01756 770199
e-mail: editor@eyespy.com
Web Site: www.eyespy.com
Office hours: 10.00am - 6.00pm Monday to Friday

USA ADDRESS: Eye Spy Magazine,
Empire State Building,
350 Fifth Ave, Suite 3304-22H, New York,
NY 10118-0069, United States of America
TOLL FREE: 877 309 9243
SUBSCRIPTION & ORDER LINE ONLY
Office hours: 7.00am - 4.00pm EST Monday to Friday

consultants, feature writers, photographers



Michael Smith
associate
editor



Kevin Coleman
USA associate
editor



Mark Birdsall
Managing
editor



Lynn Hodgson
Canadian
editor



Peter Jenkins
surveillance
editor



Nick Fielding
senior
consultant



David Hamer
associate
editor



Danny King
Security
consultant



G T Harvey
associate
editor



Donald Napier
intel news



Jim Shortt
military
consultant



Henry Hockeimer
legal
editor



Jay Goldberg
Security
consultant



Spiros Koptilos
Greece
editor



David Bickford
senior intelligence
consultant

EYE SPY MAGAZINE AVAILABLE IN 36 COUNTRIES



EYE SPY welcomes articles, photographs, case files, special reports, documents and newspaper clippings on matters featured or associated with the type of material in this magazine. Text can be submitted in most formats or hand written. If you require your submission returned, please enclose a large self addressed and stamped envelope.

The opinions and views expressed by contributors do not necessarily reflect those of the publisher or editor.

SUBSCRIPTIONS

united kingdom	\$25.00
united states of america	\$48.00
europa	\$30.00
Canada	C\$60.00
australia/middle east/asia/africa	\$30.00

please make cheques payable to:
Eye Spy Publishing Ltd

Classified Place Advertising:
UK 01756 770199
USA Toll Free 877 309 9243

EYE SPY is published eight times a year by Eye Spy Publishing Ltd. All rights reserved. No part of EYE SPY may be reproduced by any means wholly or in part, without the prior permission of the publisher. Not to be resold, lent, hired out or disposed of by trade at more than the recommended retail price.

Registered Company No. 4145 963 Registered for VAT. ISSN 1473-4362

EYE SPY functions solely as an independent, investigative and reporting organ only; it is non-political and does not discriminate against colour, race, religion or creed. Points of view to the editor please.

turtis
mag

NORTH AMERICA distribution
UNITED STATES OF AMERICA & CANADA -
Curtis Circulation Company

UK·EUROPE·ROW distribution
UK, Europe, Australasia, Rest of World
Imagine: UK 0845A 612 0094

THE INTEL RECRUITERS

COMING
SOON IN
EYE SPY

ISSUE 45 ON SALE 15 DECEMBER 2006

- PROTECTING AIRLINERS FROM HIJACKERS
- INTELLIGENCE RECRUITERS - TRADecraft
- AL-QAIDA PLANS FOR NEW UK OUTRAGE
- DANGER ON THE HIGH SEAS
- CIA AND THE UNBREAKABLE CODE
- SPYCRAFT DIY - PART 2
- THE LATEST SPY TECHNOLOGY
- TIPS FOR PROTECTING YOUR FAMILY
- THE WORLD'S GREATEST SPIES
- BIN-LADEN'S HEALTH - THE TRUE STORY



Security is no accident... it has to be practised

Support Your Local Newsagent



The best way of ensuring that you receive your copy of EYE SPY is to support your local newsagent by placing a regular standing order. The newsagent will be able to deliver it to your door or reserve it in the shop for you to collect. If you have any difficulty, why not consider taking out a post-free annual subscription - see advertisement elsewhere in this issue



Dear Newsagent,

Please reserve/deliver* a copy of EYESPY on publication, starting with the next available issue

Name Address

..... Post/Zip Code

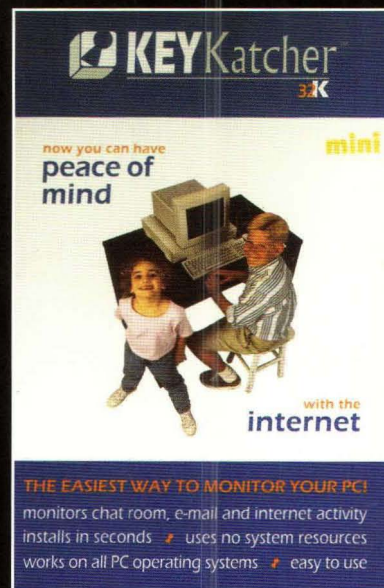
* delete where applicable

Hand the coupon in to your newsagent, or a simple handwritten note is adequate

EYE SPY INTELLIGENCE MAGAZINE

KEYKATCHER

THE WORLD'S LEADING
COMPUTER MONITORING DEVICE
AVAILABLE FROM EYE SPY



Not only is this well constructed device a valuable security tool, it is ideal for parents to protect children from the ever-present dangers on the internet. You can view all conversations and see which web sites they are visiting. E-mail and chat room activities are all captured. Although there is no "off-the-shelf" solution for effective parenting, KEYKATCHER is your eyes when you're away. It will provide you with the information you need to protect and communicate with your children.

OF COURSE IT IS MORE WIDELY USED AS A COVERT ESPIONAGE DEVICE

PORTABLE: The Keykatcher is a hardware only monitoring device. Unlike software, it can be easily moved from computer to computer. You record on one target computer, and read the memory contents on your computer. A compact size allows it to be taken anywhere. Three KeyKatchers (various capacity) are available from Eye Spy - these prices include postage and packing and air mail to America and rest of world.

- Search capability • Memory remains intact even when unplugged or during power loss • No software to install
- Virtually undetectable • 5-second installation

System Requirements: IBM PC compatible computer (Windows 98, 95, NT Linux) PS/2 keyboard connector



ES/KK2 (mini size) 32K memory £68.00 \$69.00
ES/KK4 (mini size) 64K memory £75.00 \$89.00
ES/KK5 (standard size) 128K memory £78.00 \$99.00

WORKS ON 99% OF ALL COMPUTERS
BUG DETECTORS CAN'T LOCATE

