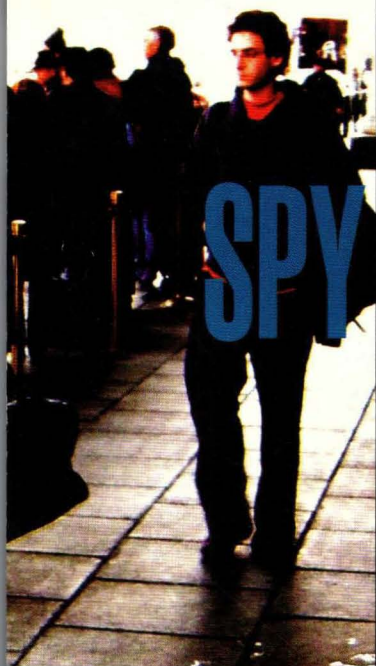


READ BY THE GLOBAL INTELLIGENCE COMMUNITY

# THE COVERT WORLD OF ESPIONAGE

# EYE SPY

## SLEEPER CELLS



## SPY TRICKS and Surveillance

## UnRestricted Warfare Threat to the USA?

## CIA FIELD STATIONS

- Lockerbie Bombing - 'New Evidence'?
- The Heroes of Flight 93
- Iraq's Uranium Hoaxers Exposed
- Vodafone Spy Phone Affair
- Red Mercury - Fact or Fiction?
- America's Agent April Fool Tricks Russians

VOLUME V NO. 40 2006  
USA \$5.99 CANADA C\$7.99

Printed in Great Britain





# INTEL FIELD STATIONS AND SPIES

Espionage and intelligence gathering conducted by officers operating in 'Field Stations'

45

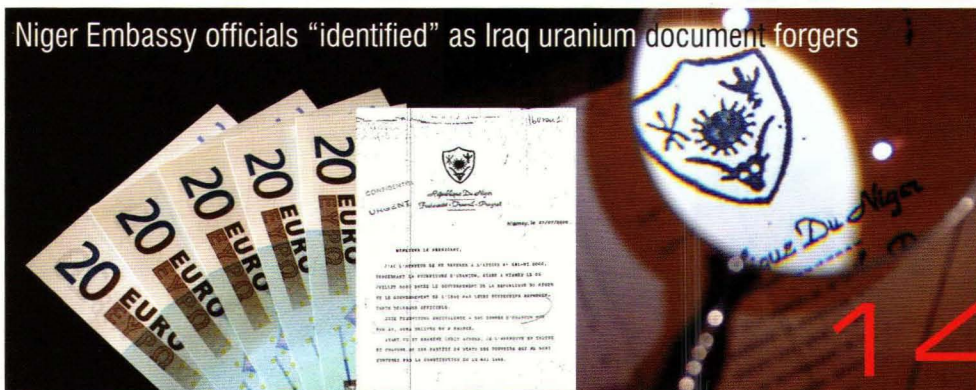
# LOCKERBIE BOMBING

34



# WHO WAS BODY 59 - DCF12?

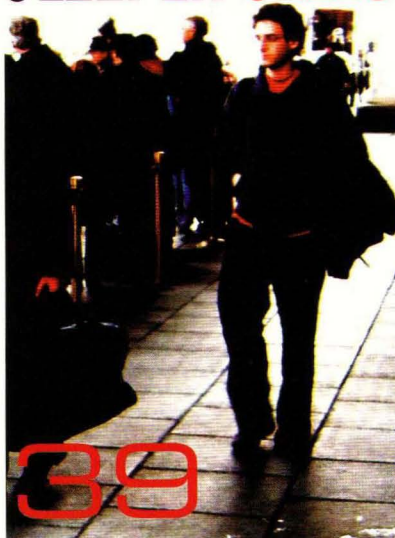
Niger Embassy officials "identified" as Iraq uranium document forgers



14

# SLEEPER CELLS

Reconnaissance and Red Flags: How security services endeavour to unlock the secrets of a terrorist operation



39

# 26 ATHENS PHONE TAP MYSTERY

Who was really behind the biggest espionage case in Greek history?



# 8 Patriot Games

British 'Spy' Shot Dead in Ireland

SAVE MONEY WITH SPECIAL READER OFFERS WHERE YOU SEE THIS SYMBOL





# EYE SPY

## C O N T E N T S

**10** Anatomy of a Hypothetical Terror Case  
FBI Director Robert Mueller provides a fascinating insight into how the security services work to investigate and capture terrorists

**18** Spy in the Camp or Agent April Fool?  
Moscow supplied Saddam with top secret Coalition invasion plans for Iraq - but was it a clever deception or genuine espionage?

**24** Britain to Introduce Terror Threat Levels  
Following the London terrorist attacks, officials have cleared the way for Britain to start using a public-orientated threat level system

**52** SpyCraft - The Watch Trick  
Eye Spy tests one of the easiest 'tricks of the trade' - using an ordinary watch piece, it is possible to gather valuable intelligence

**56** Operation Crevis  
Dubbed the 'London Bomb Plot' - an FBI informant and al-Qaida terrorist says he and members of a sleeper cell planned to strike targets throughout Britain

**58** The Public Heroes of Flight 93  
US authorities finally release Flight 93 tapes that confirm passengers did try and wrestle control back from terrorists who hijacked their aeroplane

**60** Letter from Fort Meade  
Eye Spy introduces international cipher expert David Hamer. David will provide a regular update of events pertaining to the world of codes, ciphers and machines

**67** Red Mercury Sting  
Several men have gone on trial in England. The suspects were arrested after they allegedly tried to purchase quantities of 'illusory' Red Mercury

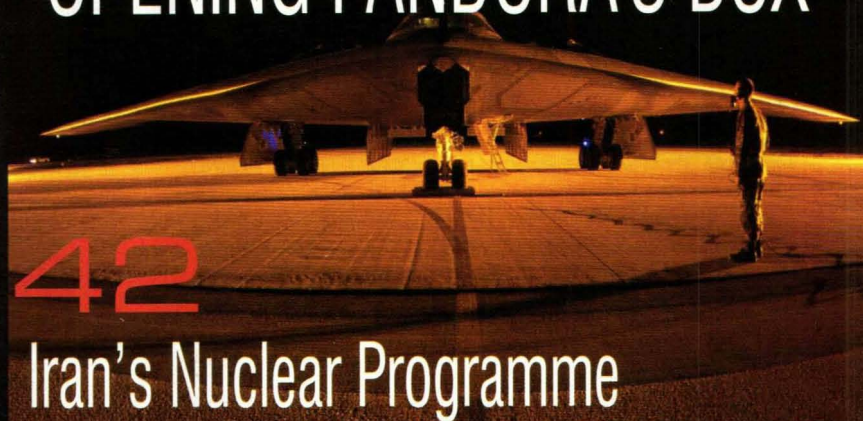
**68** UnRestricted Warfare  
US associate editor Kevin Coleman reveals methods of 'unrestricted warfare' that could force nations to their knees. Intel 'Interactive' series

**76** Mind Games



New evidence emerges that 'shadowy figures' in the intelligence world did consider bringing down the government of Harold Wilson. Secret audio recordings made by journalists in the 1970s, reveal the prime minister really feared a military coup - headed by the SAS

# OPENING PANDORA'S BOX



42

## Iran's Nuclear Programme



- 8 Denis Donaldson • 16 President Mamadou Tandja
- 18 General Tommy Franks • 26 Costas Tsalikidis • 34 Ali al-Megrahi
- 42 President Ahmadinejad • 58 Sandra Dahl • 67 Dan Brown

### some inside features

4 Intelligence Briefings; 6 MI6 advertises for recruits; 22 Trade Books; 16 Uranium sale to Iraq; 30 Back issues; 32 Eye Spy Store; 36 The Vincennes Incident; 74 Undercover - Book Releases; 80 Eye Spy Classified

## EYE SPY EDITORIAL

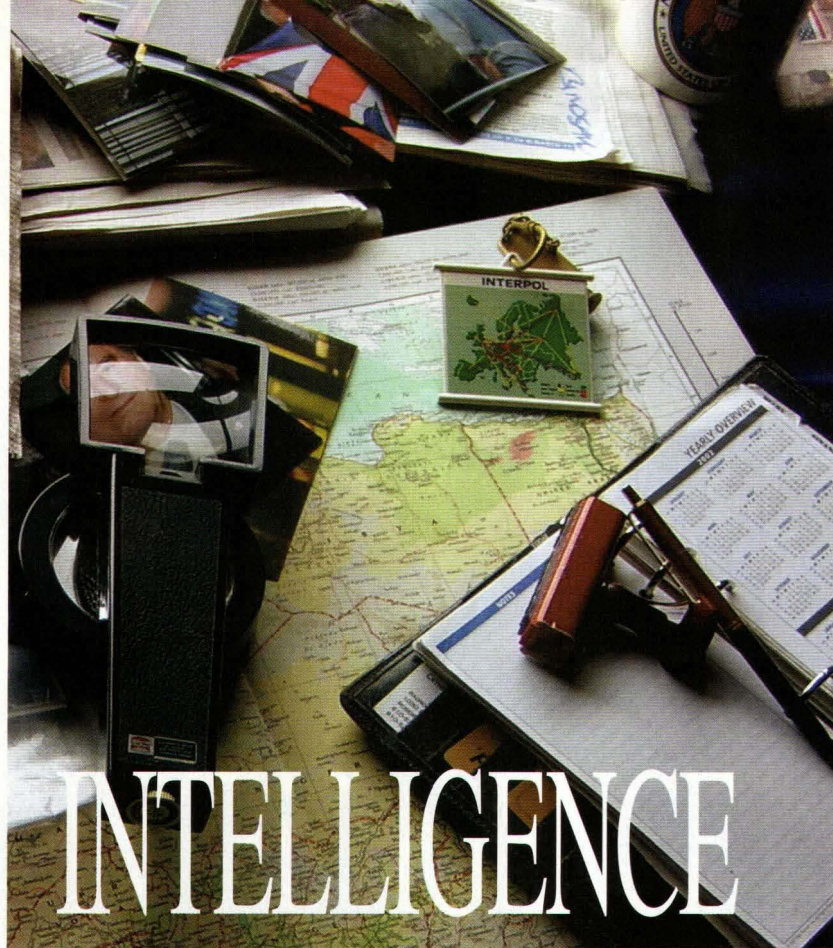
### EARLY WARNING OR PUBLICITY EXERCISE?

**E**ye Spy understands that the British Government is on the verge of introducing a terrorist 'threat system' similar to that used in the United States. Just who will decide on setting the level is at present unknown, but the intelligence services will play a role. An interesting point related to the US model concerns official statements that usually follow the raising of the level - "the public are usually assured there has been no specific threat." This has confused many in the media who have been politely rebuffed when questioning the decision. "Something" must have nudged the security services or why raise the bar?



The UK move follows a series of awful government decisions to change the current warning level prior to, during and just after two sets of terrorists attacked London in July 2005 (see page 24). And though the move will be generally welcomed by the public, what happens if an attack occurs when the threat model is set at low? Criticism again, I'm sure. The truth is, terrorists operate outside the law and use stealth tactics to defeat security efforts. They never advertise their intentions. However, a threat warning system should remind people to be vigilant at all times. Public apathy is a vital tool used by terrorists. The new system will appear first on all government web sites, but I suspect it won't be too long before a chart, or 'traffic light' arrangement features in newspapers, bill board adverts etc.





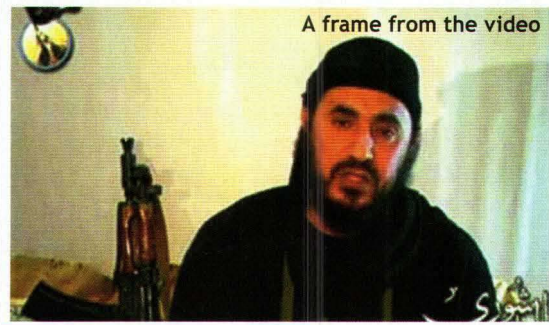
# INTELLIGENCE

## AL-ZARQAWI IN VIDEO THREAT

**IRAQ:** On April 25, one of the world's most wanted terrorists, Abu Musab al-Zarqawi, made a rare appearance in a 35-minute video. In the tape, he denounced the new Iraqi government and warned of more attacks. The video came just two days after an audio taped message from Osama bin Laden was aired and just hours after suicide bombers struck in Egypt killing 20 people.

"This democratic play which you brought to Iraq after you promised people freedom and... economic stability has gone with the wind," Zarqawi said. "Today, you are trying with all means to assemble people who differ among themselves... and apostates to form a government to save you from your critical situation."

Intelligence analysts are unsure if the video was made in Iraq or a neighbouring country.

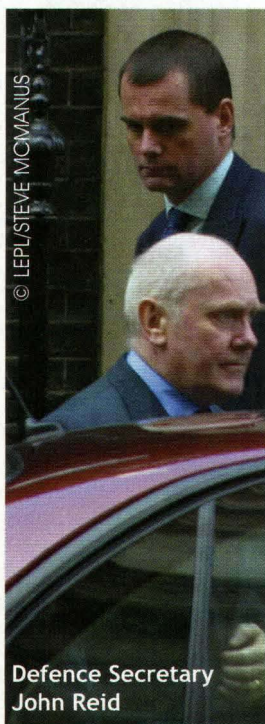


## UK Counter-Terrorism Centre Unveiled

**T**he UK has established an elite new centre that will "co-ordinate the government's technical response" to terrorism, both in Britain and abroad. The Ministry of Defence (MOD) Counter-Terrorism Science and Technology Centre will be staffed by a variety of experts from government, industry and academia.

Intelligence sources say the move is a direct result of the London terrorist attacks in July 2005, the increasing problems posed by improvised explosive devices, chemical and biological threats and suicide bombers. Besides research into counter-measures' technology the centre will help identify and respond to a variety of general terrorist operations. Its science wing will help develop new technologies that can be

quickly assigned to all parts of the UK and beyond. The centre will also be used to augment existing high-end projects including UAV (unmanned aerial vehicle) programmes and transport security.



Defence Secretary John Reid

Defence Secretary John Reid said the unit would be a "world class hub."

The centre will not just co-ordinate and control the science and technology that underpins the MOD's counter-terrorism activity, but also provide a 'one-stop shop' for other government departments who use MOD expertise to tackle domestic terror threats. Intelligence services such as MI5 and MI6 will be able to use the services of the facility, though the police and British armed forces will also have full access. It will be based at the Defence, Science and Technology Laboratory in Porton Down, Wiltshire.

Defence Secretary John Reid said: "Terrorism is a real threat to us all and we must do everything we can to ensure the UK is best equipped to deal with any

incident both at home and wherever our Armed Forces deploy.

"This new centre will provide a world class hub to ensure government laboratories, industry and

academia are used as efficiently as possible to enhance innovation and keep one step ahead of evolving terrorist threats."

It is understood the centre will start operations with a





# Russia's Truth Verifiers

## Airline passengers face lie detector tests

**T**ourists, businessmen and most airline passengers travelling through Russia, will soon face new security measures, including a lie detector test. The machines - dubbed "truth verifiers" - will be introduced at Moscow's Domodedovo airport this summer. Passengers will be invited to pick up a hand set and respond to a series of questions. One question

relates to your identity, and another asks if you are carrying weapons, drugs etc. Security officials are confident that the technology will help identify terrorists and drug smugglers.

Developed by an Israeli company, the lie detectors appear to work by identifying if the response is from the person's "imagination" or "memory." Project testing

will be selective at first (only those deemed suspicious by security officials), but if successful may become mandatory for everyone.

"We know that this could be uncomfortable for some passengers but it is a necessary step," said Vladimir Kornilov, the IT director for East Line, which operates the airport. "If a person fails, he is accompa-



nied by a guard to a cubicle where he is asked questions in a more intense atmosphere," Mr Kornilov said.

Critics say the test will create long queues, but officials say passengers will be asked the question when

baggage, shoes and other items pass through the airport x-ray machine.

Eye Spy understands the devices are already being used by major insurance firms to help determine if some claims are fraudulent.

THE MOST CONTROVERSIAL BOOK OF 2006

*The unit so secret it doesn't even have a name*

Available from Eye Spy

KILLER ELITE

Ref: ES/1141

UK £22.49 USA \$48.00  
ROW £24.99

Use order form on page 82

team of about 15-20 specialists, though this is certain to rise. Commenting on the move, Centre director Ken Brigden said: "As threats against the UK Armed Forces are becoming



increasingly sophisticated and diverse, science and technology advice plays an even more crucial role in the planning and preparation of military operations.

"This centre will be staffed by the very best MOD, academic and industry counter-terrorist technical experts with cutting edge expertise in chemical, biological, radiological, nuclear and explosive threats. Terrorist threats evolve rapidly so the centre will respond, not just to current threats but also anticipate threats as they emerge and develop."

COURTESY: MINISTRY OF DEFENCE

## UN DIRTY BOMB FEARS



**O**fficials at the United Nations nuclear watchdog have issued a report warning of a sharp increase in the smuggling of radioactive material that could be used in a terrorist 'dirty bomb'.

A report reveals that the illegal movement, possession or loss of radioactive sources has doubled from 2002 to 2004, according to the International Atomic Energy Agency. About half the cases involved criminal activity.

The fear of a terrorist attack involving a dirty bomb has

long been a concern to many governments, especially as they require only radioactive material and a small detonator. The explosion would not necessarily result in an immediate loss of life, but the resultant contamination would create huge areas that are inaccessible. Al-Qaida has openly declared its intentions to use such weapons in financial areas and centres of population.

Groups operating under the al-Qaida umbrella have been accused of obtaining radioactive materials in Chechnya and other former Soviet Bloc countries.



Analysts warn that significant amounts of material that can be used in dirty bombs, is unaccounted for in hospitals, factories and holding facilities.

## Israel's New Spy Satellite

**O**n 25 April, Israel successfully launched Eros B - a highly advanced spy satellite that will enable it to monitor Iran's nuclear programme. Eros B, launched from the Svobodny Cosmodrome in the Siberia using a Russian Start-1 rocket. Equipped with highly-sensitive equipment, the satellite can document the most minute details on the Earth's surface. Its cameras can record objects only 70 centimetres in size. Tel Aviv hopes to gain more detailed

information on Iran's nuclear programme and on its long-range missiles from the satellite.

Asked about its potential to spy on Iran, an Israeli official said: "The capabilities of the satellite speak for themselves. I do not need to say anything about what the purpose of its use might be."

Eros B will join an earlier version of the satellite, launched in December 2000. Both are set to augment the



work of Israel's declared spy satellite, Ofek 5, which regularly passes over the Middle East.



# NOT SO SECRET

## MI6 Advertises for New Recruits... in The Times

Not that everyone need apply, but Britain's Secret Intelligence Service, better known as MI6, broke a near 100-year old tradition by actually advertising for staff! On 27 April, The Times ran MI6's inaugural advertisement accompanied by a number of photographs that featured exotic locations, from the Middle East to Africa. It is just another example that the world's most secret service is prepared to show a 'human touch'.

All applicants must be British, resourceful, in good health and be able to keep a secret.

Last year the agency launched its own web site, a move deemed "extraordinary" by some. Now it is searching for new personnel - "thoroughly efficient administrators, analysts, linguists, information technology experts, as well as operational officers". A number of recruits will undoubtedly find themselves gathering intelligence in overseas countries,

though most will work at MI6's London headquarters. The 'operational officers', - a candid phrase for spies - also need a university degree, strong intellectual skills, an interest in foreign cultures and an "out-standing ability to persuade and to influence".

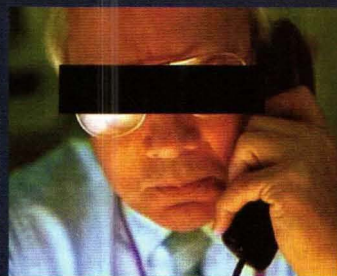
In days gone by, those charged with the delicate task of espionage were often recruited from the ranks of Britain's academia - Oxford and Cambridge universities come to mind. Postal applications to join MI6 were usually torn up even before the sender's name was read. How things have changed.

While the move is surprising, it is not totally unexpected. MI6 is facing huge challenges, not least that posed by al-Qaida - just one of many emerging international terrorist groups. With Iran on the verge of creating a nuclear device, and other nations moving into this area, officials believe that a more versatile and dynamic service must be created.

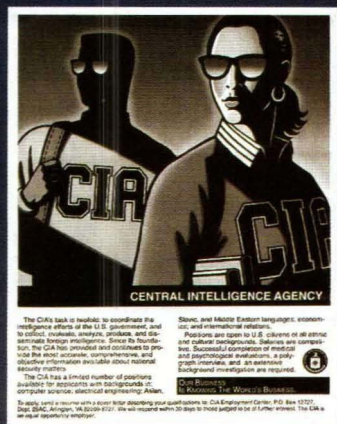
Since October 2005, its web site has had a section on recruiting. However, the newspaper advertisement is the beginning of a new phase in trying to secure the services of Britain's 'finest'. It says the agency operates around the world to make Britain 'safer and more prosperous' and hires 'people we can depend on because everyone in the UK depends on them'.

MI6 is now reaching out to the public, a move initiated to create a more "user friendly" organisation. Notwithstanding that, it is interesting to note that the initial adverts appeared only in The Times and Economist.

Unlike recruitment during the Cold War and earlier, MI6 does face the prospect of a potential terrorist joining the service. Yet the vetting is extremely tough and it is highly unlikely those intent on double dealing, would pass the first of many interviews and exam stages. For those genuine applicants, MI6, like its



sister organisation MI5, warns against telling anyone other than a spouse or closer partner that they have applied... just in case you are accepted.



MI6's American counterpart - the CIA has never been shy to advertise - as this poster shows

"Staff who join SIS can look forward to a career that will have moments when the gap narrows just a little and the certainty of a stimulating and rewarding career which, like Bond's, will be in the service of their country..." MI6 Advert





# EYE SPY



INTERNATIONAL INTELLIGENCE EXTRA

# CIA SPY FLIGHTS

## Former CIA Officer Denies Leaking Spy Flight Intelligence

**A** solicitor representing fired CIA officer Mary O. McCarthy said his client did not leak any classified information and did not disclose to *Washington Post* reporter Dana Priest, the existence of secret CIA-run prisons in Eastern Europe for suspected terrorists. The statement by Ty Cobb, a lawyer in the Washington office of Hogan & Hartson who said he was speaking for McCarthy, came as a senior intelligence official said the agency is not asserting that McCarthy was a key source of Priest's articles last year disclosing the agency's secret prisons.

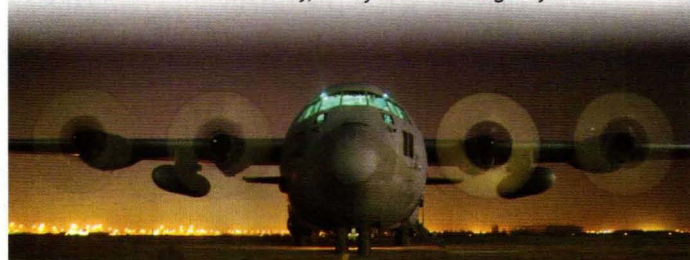
McCarthy was fired because the CIA concluded that she had undisclosed contacts with journalists, including Priest, in violation of a security agreement. That does not mean she revealed the existence of the prisons to Priest. Cobb said that McCarthy,

who worked in the CIA inspector general's office, "did not have access to the information she is accused of leaking," namely the classified information about any secret detention centres in Europe.

Intelligence officers often have contacts in the media world, but it is still a violation of the CIA's rules.

Priest's articles resulted in a major internal CIA investigation that included polygraphing numerous officials who could have had access to the intelligence, including McCarthy.

McCarthy, 61, who had previously held senior posts at the White House and the National Intelligence Council (NIC), said she was "devastated." She was due to retire just days before she was sacked after serving more than 20 years in the agency.



## EUROPE FULLY AWARE OF SPY FLIGHTS

**BRUSSELS:** An investigation, details of which were released in April, by the European parliament, said the CIA has operated more than 1,000 secret flights over EU territory in the past five years. Many of these were used in the practice known as 'extraordinary rendition' - transferring suspected al-Qaida terrorists for interrogation. The report's author, Italian MEP Claudio Fava (below) suggested some EU

governments knew about the flights.

"After 9/11, within the framework of the fight against terrorism,

the violation of human and fundamental rights was not isolated or an excessive measure confined to a short period of time, but rather a widespread regular practice in which the majority of European countries were involved," said Mr Fava, a member of the European parliament's left wing socialist group.



## LONDON TERRORIST PLOT

**F**ive men have denied plotting to kill and cause explosions on London's Underground transport system on 21 July last year. The men also denied various charges of possessing an improvised explosive device (IED) and four denied attempted murder. The trial date has been set for 3 October 2006.

A sixth man, Adel Yahya, 23, from London, was remanded to another hearing in June. He was charged with conspiracy to cause explosions likely to endanger life but did not enter a plea. Muktar Said Ibrahim, 27, Ramzi Mohammed, 23, Yassin Omar, 24, Manfo Asiedu, 32 and Hussain Osman, 27, all from London, entered pleas before the trial judge, Mr Justice Fulford, at The Old Bailey. All denied two charges of conspiracy to murder and conspiracy to cause explosions likely to endanger life between January 1 and July 30 last year. They all pleaded not guilty to individual charges of having an improvised explosive device with intent to cause an explosion likely to endanger life on July 21 last year.

The men were arrested after bombs hidden in rucksacks failed to detonate.



## NSA OVERLOAD

**9/11 eavesdropping intelligence 'overwhelmed FBI' claim some agents**

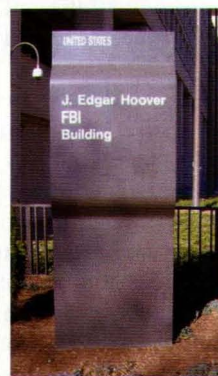
turned its attention to outgoing and incoming communications' traffic to ascertain terrorist activity within the USA. Within weeks the agency had provided a plethora of intelligence on hundreds of people that had received, or made, "suspicious calls."

Now some former FBI agents have complained that in most cases the intelligence led them nowhere and was confusing in that it lacked substance.

A former officer speaking on the condition of anonymity

said "we didn't really know what we were looking for."

NSA intelligence in the form of e-mail messages and telephone messages resulted in hundreds of FBI surveillance operations and enquiries. In one month alone, some 2,000 signals were delivered to the FBI who appointed hundreds of agents to investigate. Some of those involved with data examination said that most led to "dead ends." It has been alleged that the FBI "complained" to the NSA that the data was simply too much to handle.



**T**he row over the NSA's secret US-based eavesdropping programme has prompted some former FBI officers to complain that the information they received from the spy agency was often spurious and overwhelmed local offices. Following the attacks on New York and Washington, the NSA



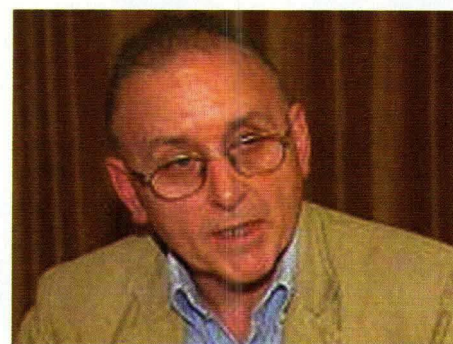
# Patriot Games

## British 'Spy' Shot Dead in Ireland

### GOVERNMENT DENIES BRITISH INTELLIGENCE BEHIND SHOOTING

**D**enis Donaldson, a former senior Sinn Féin politician who recently admitted spying on the IRA and his own colleagues for more than 20 years, was found dead on 4 April. He had apparently been shot twice with a shot gun at a remote farmhouse near Glenties, Co Donegal, owned by his son-in-law, Ciaran Kearney. Donaldson was killed after he answered a knock on his front door. In December 2005, Donaldson, also a former IRA volunteer, caused mayhem in the intelligence world when he told reporters that he had worked for years as a 'British intelligence asset'. Sinn Féin promptly expelled its former head of administration at Stormont, the seat of power in the North of Ireland.

The incident is the culmination of an affair that began four years ago, when it was alleged the IRA had been running a spy ring inside Stormont. Donaldson, head of administration, along with two other men, was named as being part of a major espionage operation against the government. The three were arrested and charged after police seized documents and computer discs in a raid on Sinn Féin's offices at Stormont on 5 October 2002. The British government then suspended devolution, embarking



Denis Donaldson

on three years of direct rule, after the DUP and the Ulster Unionists threatened to collapse the Executive with resignations.

Peter Hain, the Northern Ireland Secretary said "something like 1,000 documents were stolen from the Northern Ireland Office. They disappeared. They were stolen." However, without warning, the Director of Public Prosecutions in Northern Ireland said the case against the three men was closed. Sinn Féin said this was "proof enough" that the IRA 'spy ring' was a British fabrication. What followed was even more remarkable; seven days after he was cleared, Donaldson, 55, declared he had been spying for British Special Branch against Sinn Féin (and the IRA), since the 1980s. Donaldson himself described the Stormont spying allegations as a sham. He "deeply regretted his activities with British Intelligence and RUC/PSNI Special

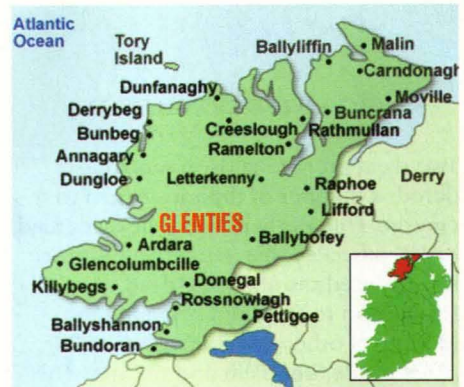
Stormont







Irish security services  
have launched a  
major investigation

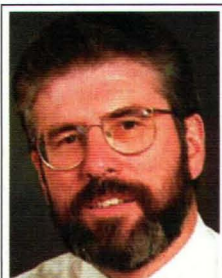


we published the story and I got the impression that he had been ordered there." He was then offered protection by Irish and British police, but apparently refused. ➤

Branch" and he apologised to anyone who has suffered as a result of his activities.

The surprising announcement came as a shock to the IRA and many intelligence watchers, for though it was acknowledged that British intelligence had infiltrated Sinn Féin and the IRA at many levels, few had any idea that it had an informant at the very heart of the movement. According to Sinn Féin leader Gerry Adams, the PSNI (Police Service Northern Ireland) had quietly told him that Donaldson was going to be "outed as an informer" before he could make the announcement himself. They also stated that his life was in danger.

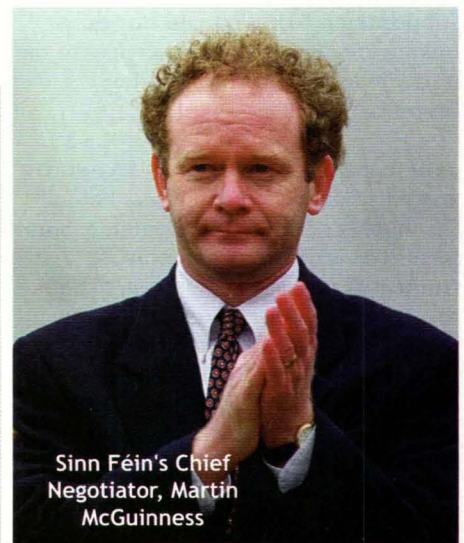
Questions were asked by both sides. Just what intelligence had Donaldson provided to MI5 and MI6, and how was it possible to remain undercover for such a great length of time? Senior intelligence sources say that assets such as Donaldson are not there just to pass on information, they are there to "influence strategy and direction at the highest level."



Sinn Féin  
President Gerry  
Adams vehemently  
denounced  
shooting of Denis  
Donaldson

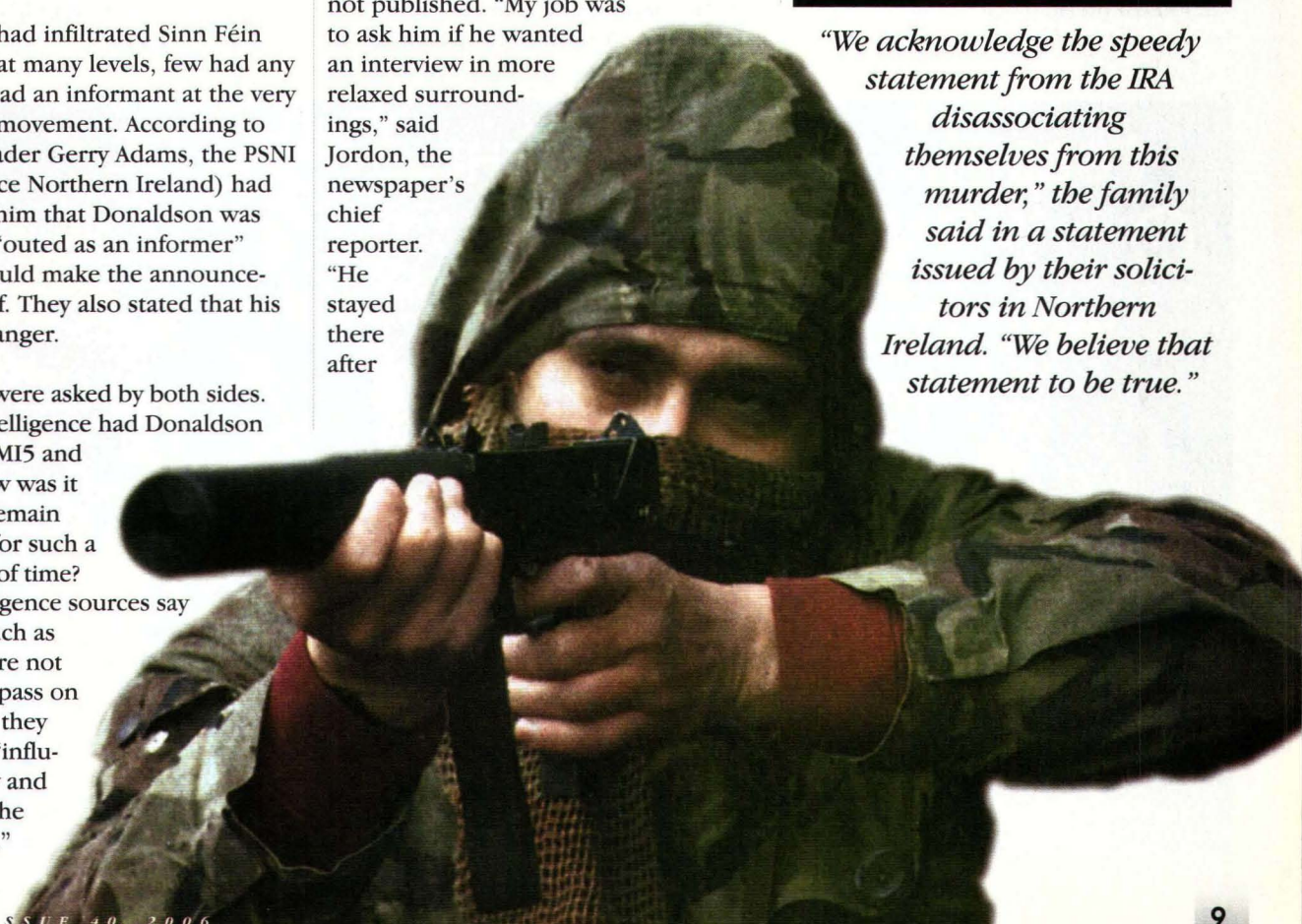
Commenting on the spying, Alex Attwood, of the nationalist SDLP, said: "Elements in the British system and Provisional movement are partners in a dirty peace. They spy on each other and they cover up for each other."

Following the revelation, Donaldson moved from the north in January to a secret location in the Irish Republic along with his family. That location was discovered by Hugh Jordon, a journalist from the *Sunday World*. He defended a resultant article and said the exact location of Donaldson's farmhouse was not published. "My job was to ask him if he wanted an interview in more relaxed surroundings," said Jordon, the newspaper's chief reporter. "He stayed there after



Sinn Féin's Chief  
Negotiator, Martin  
McGuinness

*"We acknowledge the speedy statement from the IRA disassociating themselves from this murder," the family said in a statement issued by their solicitors in Northern Ireland. "We believe that statement to be true."*





## WHO KILLED DONALDSON?

Two days after Donaldson was murdered, a number of theories began to emerge. One of them was quickly denied by UK officials - that British intelligence had ordered the shooting dead of Donaldson to stop him revealing the identity of other possible agents still in place inside Sinn Féin and the IRA. The finger of blame has also been pointed at hard-line dissident republicans opposed to the peace process, a view supported by Peter Hain. "I have obviously consulted with the security services and police. Nobody at the minute has any idea as to how the murder took place or who was responsible. The investigation by Irish police is continuing and we are supporting it." He also said stories linking the British security services to the murder were "fanciful and rather desperate."

For its part, the Provisional IRA issued an immediate denial that it was behind the murder of the former comrade. Sinn Féin's Chief Negotiator, Martin McGuinness, said he was very angry about the killing of Donaldson. Speaking to RTE News, he described the death as an attack on the peace process. McGuinness said Sinn Féin absolutely dissociated itself from the killing and said whoever carried it out was hostile to the concept of peace in Ireland.

Sinn Féin president Gerry Adams said he was not prepared to speculate on



Garda forensic specialists carried out meticulous search for clues

who might have been responsible. But he added: "It has to be condemned. We are living in a different era, and in the future in which everyone could share. This killing seems to have been carried out by those who have not accepted that."

The timing of the murder - just two days before a meeting between British and Irish heads of government may also be significant. The leaders were involved in talks to persuade the province's politicians to share power.

### WEAPONS OF CHOICE

Shotguns are the preferred weapons used by paramilitary gunmen. They are called 'clean weapons' because forensic



Weapon that killed Mr Donaldson was almost certainly a shotgun

specialists find it more difficult to trace the shot, compared with bullets fired from pistols or rifles. Following his death, there were reports Donaldson's right hand had been cut off. However, intelligence sources told Eye Spy this had been caused as he attempted to stop the gunman gaining access through the front door.

Chief Superintendent Terry McGinn vowed yesterday that no stone would be left unturned in the search for those responsible.

## FORENSIC BULLET MATCHING

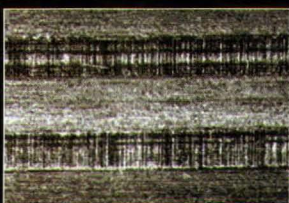
Certain parts of a firearm mark the bullet and cartridge. Rifling gives the bullet a signature marking that is unique to the weapon that fired it. Rifling exists as part of the manufacturing process of the firearm and serves to put spin on the bullet, giving it a straighter trajectory (much the same way as an American football quarterback puts spin on a ball). Rifling consists of lands and grooves that spiral down the gun barrel (think of the seam on a paper towel tube). When the gunpowder in the cartridge is ignited, it forces the bullet



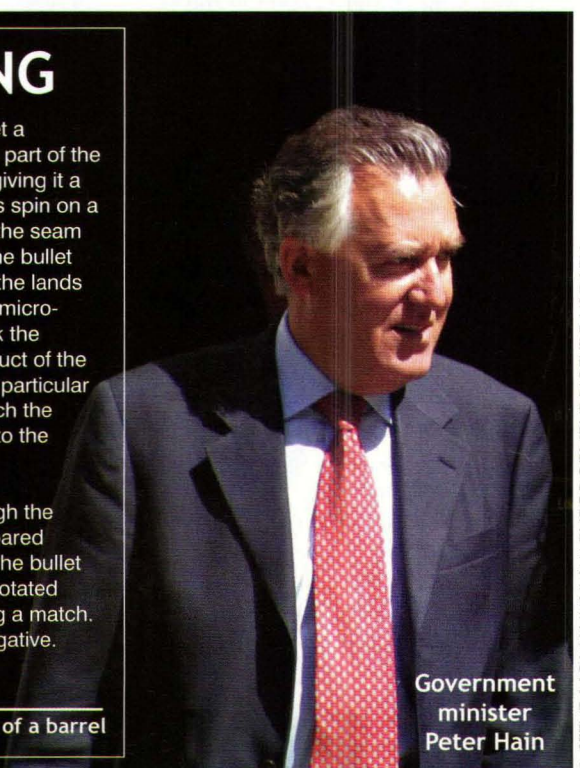
Rifling on a fired bullet

down the gun barrel, expanding the soft lead into the lands and grooves. As the bullet passes down the barrel, microscopic scratches from the lands and grooves mark the bullet. These microscopic scratches are a by-product of the manufacturing process and are totally unique to a particular firearm. Thus, the scratch marks on the bullet match the scratch marks in the barrel of the gun that fired it, to the exclusion of all other weapons.

This is tested in the lab by test firing a bullet through the suspect weapon. The test fired bullet is then compared under a comparison microscope, side by side, to the bullet recovered from the crime scene. Both bullets are rotated until the striations can be made to line up, showing a match. If the striations cannot be lined up, the result is negative.



Microscopic view of imperfections in the rifling of a barrel



Government minister Peter Hain



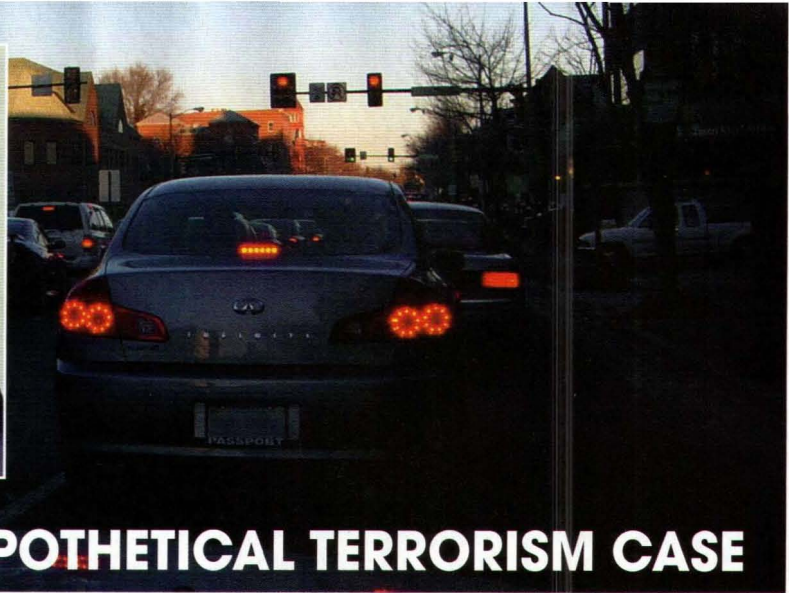
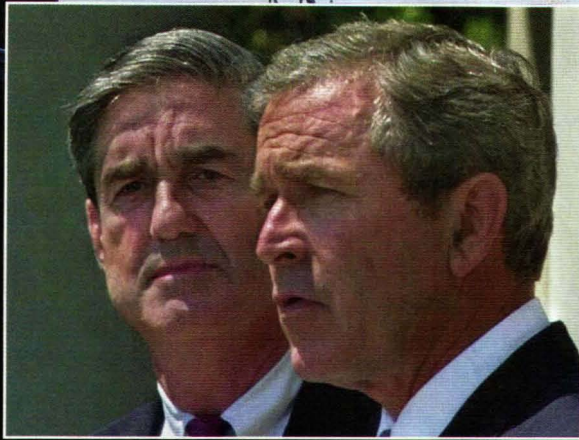
# FBI ANATOMY

## EXAMINATION OF A HYPOTHETICAL TERRORISM CASE



FBI Director Robert Mueller recently delivered a lecture that provided a fascinating insight into how the FBI investigates suspected terrorist situations. The effort often involves working with a variety of local authorities and international law enforcement agencies. To explain (and simplify) the often complex work of investigators, Mr Mueller created a hypothetical case... ➤





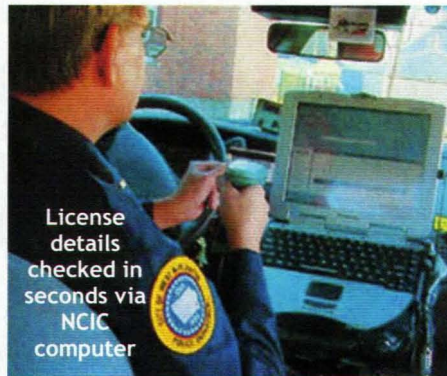
## FBI ANATOMY OF A HYPOTHETICAL TERRORISM CASE

**T**he hypothetical case begins with 'Officer John Smith' of the Houston (Texas) Police Department.

Officer Smith checks his secure LEO (**Law Enforcement Online**) computer account before going on duty. He reads an FBI/Department of Homeland Security Intelligence Bulletin that notes certain Europeans associated with a recent terrorist attack may be living in the United States. The suspects reportedly called phone numbers in the USA with pre-paid cell phones. Enquiries reveal that they had been purchased from a cell phone shop in Texas.

While on duty, Smith sees a car speed through a red light in Houston city centre. He orders the car to pull over, and asks the driver for his license and registration. He runs the license, license plate, and registration information through his patrol car NCIC (**National Crime Information Center**) computer and instantly learns the car has been reported as stolen.

Moments later Smith gets an alert on his computer from TSC, the **Terrorist Screening Center**: the driver's name is on a terrorist watch list. Smith calls the facility to get the full report *as well as* guidance on what questions to ask the driver.



The driver claims he's a student from Europe studying at the local university and simply sightseeing. Smith looks hard into the car and spots several cell phones, a camera, and a map piled on the front seat. "What's that map?" he asks. The driver hands him the map.

Smith notes circles drawn around a sports stadium, a hospital, a shopping centre, and the port. Immediately Smith places the driver

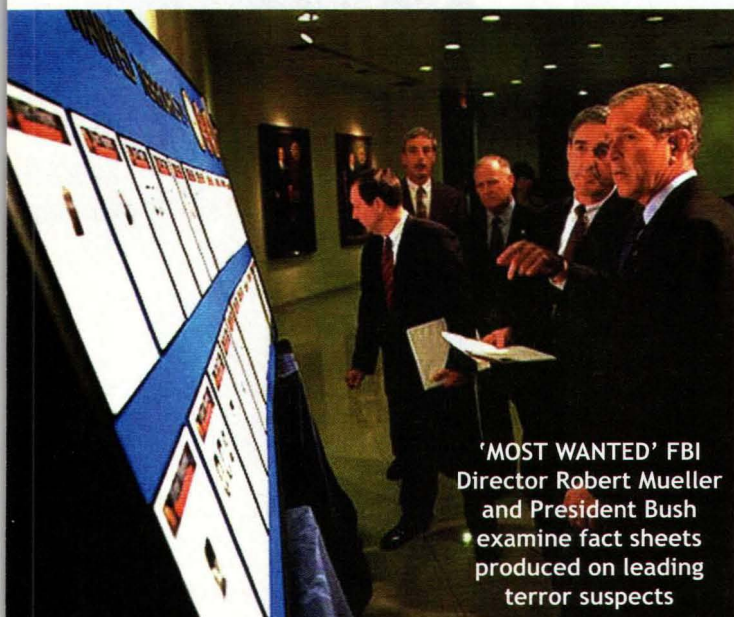


under arrest for possession of a stolen car and takes him to the police station for questioning.

At his first opportunity, Smith telephones a police colleague serving on the FBI's JTTF (**Joint Terrorism Task Force**) in Houston and asks her to check State Department databases.

Other officers at the station take the driver's fingerprints. These are then entered into the IAFIS (**Integrated Automated Fingerprint Identification System**) database. The system produces a match - the driver has been arrested before, but under another name.

The telephone rings - it's Houston JTTF: "Yes, the driver **IS** in the United States on a student visa, but is **NOT** enrolled in any university."



'MOST WANTED' FBI Director Robert Mueller and President Bush examine fact sheets produced on leading terror suspects

### LAW ENFORCEMENT ONLINE

Following the first London bombing in July 2005, the FBI notified more than 5,000 law enforcement professionals nationwide about the attacks in 32 seconds. Law Enforcement Online, or LEO, is a secure computer network that gives law enforcement officers around the United States access to sensitive but unclassified information, intelligence reports, and alerts crafted by bureau agents and analysts. The FBI say it is information "our partners need quickly, but shouldn't be available to the public." LEO started ten years ago as a small dial-up service with just 20 members. Today it has more than 46,000 members nationwide.

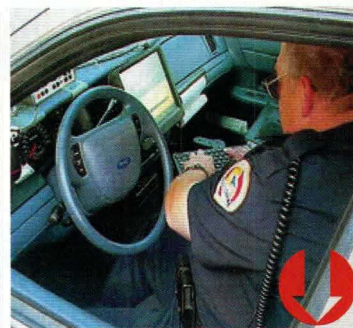




Officer Smith checks his secure LEO (Law Enforcement Online) computer account before going on duty - learns of terror attack in Europe



Smith sees a car speed through a red light in Houston city centre. He orders the car to pull over



NCIC (National Crime Information Center) computer confirm car has been reported as stolen - driver arrested



Details of case circulated via computers to FBI overseas offices and international agencies



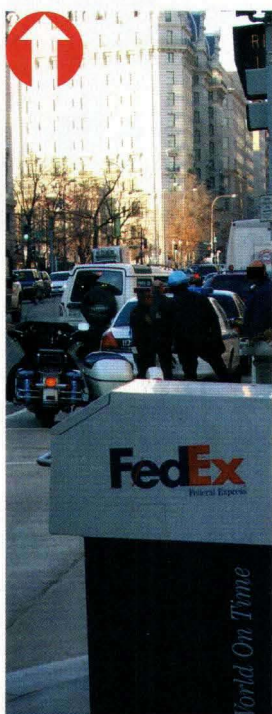
Terrorist Screening Center reports the driver's name is on a terrorist watch list

**SEEKING INFORMATION**

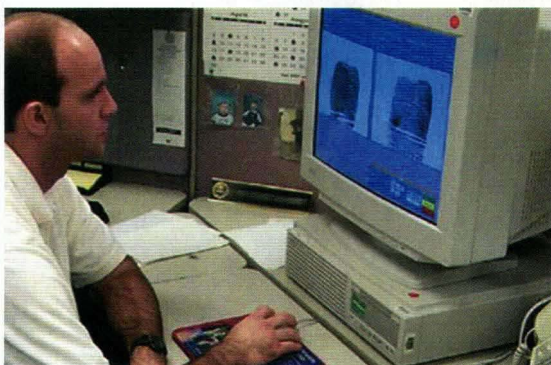
War on Terrorism



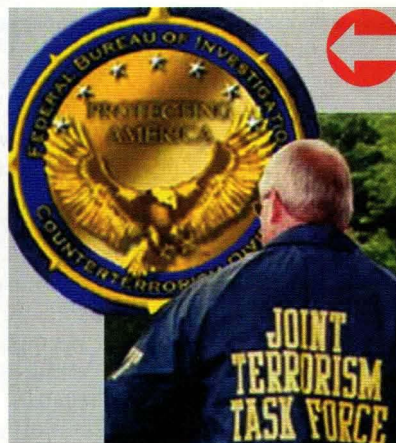
## HOW IT WORKS



Cell phone information links driver to European terrorist attack



Driver's fingerprints entered into the IAFIS (Integrated Automated Fingerprint Identification System) database which produces a match



Smith telephones a police colleague serving on the FBI's JTTF (Joint Terrorism Task Force) in Houston and asks her to check State Department databases

Back to TSC: Is there a 'hit' on its databases for the alias of the driver? YES.

The TSC FBI Agent runs the cell phone information through investigative databases and finds one of the phones was called from a phone connected to the very European terrorist attack Smith had read about just hours before. The TSC agent advises he's already alerted **FBI Legal Attaché** offices in Europe and advised

USA and European law enforcement and intelligence agencies of the incident. These services are now fully conversant with developments. Liaison and cooperation can start apace.

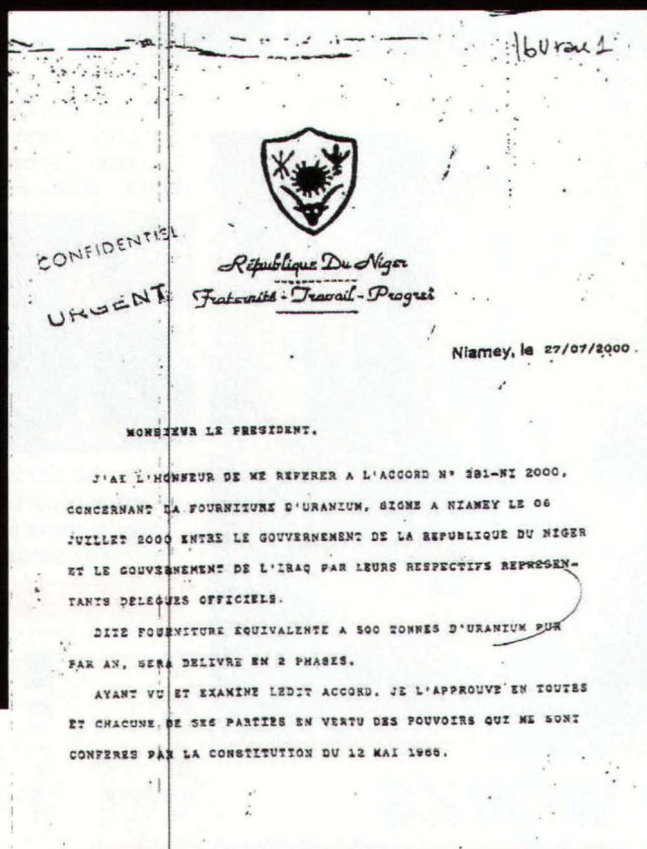
Director Mueller notes: "And so, within hours of the arrest, the Houston Police Department, the FBI, the CIA, and European law enforcement and intelligence agencies are working hand-in-hand on this investigation. Has the man been sent to the United States to

do reconnaissance on possible targets? Or is he here to recruit members for a terrorist cell? As the pieces of the puzzle come together, it becomes clear that the work of just one police officer set in motion a chain of events that led to an international investigation, the identification of a potential terrorist cell, and the prevention of a possible terrorist attack."





# Yellow Brick Road



## Niger Embassy officials identified as Iraq uranium document forgers

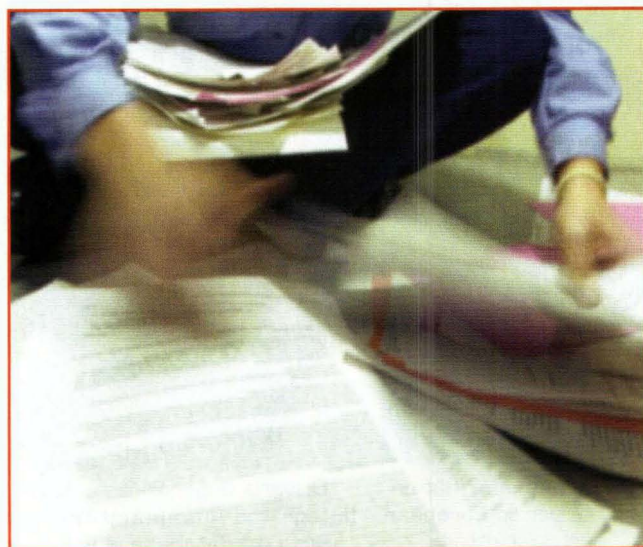
**A**ccording to *The Sunday Times* investigative journalist and Eye Spy associate editor Michael Smith, NATO sources said two members of staff at Niger's Italian embassy were behind the bogus documents - used in part to justify the war in Iraq. An investigation has allegedly revealed that Niger's consul Adam Maiga Zakariaou, and the ambassador's personal assistant Laura Montini, created a 'contract document' in 2002 that showed Saddam Hussein had purchased yellowcake (uranium ore) from their country.

Though the 'Niger Documents', as they have since become known, have been dismissed as "poor forgeries", investigators are keen to discover the background of their origin, not least because several shadowy figures in the intelligence world became involved in the affair. Rumours abounded that they were forged by the CIA and MI6 (with a little help from SISMI - the Italian intelligence service) to help build the case for war. There was even a story that France's intelligence service, the

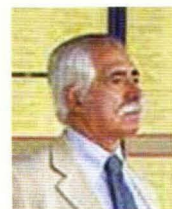
DGSE, wanted to embarrass Washington and London as war loomed with Iraq.

In the end, it seems the lure of money prompted the two embassy officials to embark on the mission. Amidst reports of genuine intelligence that Saddam had sent officials to Africa to examine the possibility of acquiring uranium ore, the two Niger officials allegedly doctored an authentic contract. The finished article showed a government agreement between Iraq and Niger discussing the supply of 500 tons of yellowcake.

Michael Smith has learned that the genesis of this extraordinary incident began in a Rome bar in February 2000. A meeting was arranged by Antonio Nucera, an officer in the SISMI, and two of his former agents, Rocco Martino and Laura Montini. Martino was somewhat of a controversial character, an ex-police



officer with lots of links to the intelligence world. At the time, SISMI had no idea Martino was also on the books of France's DGSE being paid a "retainer" of about £1,000 a month. "Nucera asked if I was interested in meeting a person who worked in an African embassy and who had been able to supply [Nucera with] documents and information, including the embassy's cipher," Martino told an investigating magistrate during an Italian inquiry. Laura Montini allegedly



Rocco Martino





# MONEY "PRIMARY INCENTIVE" FOR ELABORATE HOAX

accepted about £300 a month to work as Martino's 'sub agent'.

Shortly thereafter, Montini handed Martino details of a visit to Niger by Wissam al-Zahawie, Iraq's ambassador to the Vatican. This was key intelligence, as France, who controlled much of the yellowcake mining in Niger was monitoring sales to overseas countries. Martino passed the information to his DGSE controller. Paris wanted further details and asked him to try and get any sort of documentation. "Martino told me that if he was able to obtain a copy of a contract then he would have earned a lot of money from an unspecified 'intelligence' organisation," she told the Italian magistrate. "She was [the ambassador's] trusted personal assistant. The consul Zakariaou... needed money. He would help her forge the documents," NATO sources claim. Unfortunately for all parties concerned, DGSE analysts soon spotted numerous errors in the contract and refused to hand over an agreed fee.

A surprising turn of events in 2002 complicated the situation. Another letter, (believed genuine by Britain's Butler inquiry into Iraq intelligence) reportedly

from al-Zahawie, referred to a visit to Niger in 1999. That mentioned the possibility of Niger supplying uranium to Iraq. There was no evidence the African country had agreed to a sale, but the content was such that it indicated Saddam was interested in acquiring the yellowcake. The DGSE told MI6 who forwarded a copy of the document to the CIA. In January 2003, President Bush declared that the "British had learnt that Saddam Hussein recently sought significant quantities of uranium from Africa." The CIA had actually pressed MI6 to discover the DGSE source, but the French wanted to "protect its source" - Martino.

Ultimately Martino touted the faked documents elsewhere and they soon appeared in the Italian magazine *'Panorama'*. Journalist Elisabetta Burba soon realised they were bogus and handed a copy to officials at the US Embassy in Rome in October 2002. She asserts that she received seventeen pages of documents and a Niger codebook from 1967.

Michael Smith writes: "Zakariaou, now a Niger representative to the United Nations Food and Agriculture Organisation in Rome, said: 'If you really want the

truth you must look somewhere else. You should deepen your inquiries elsewhere'."

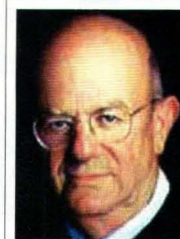
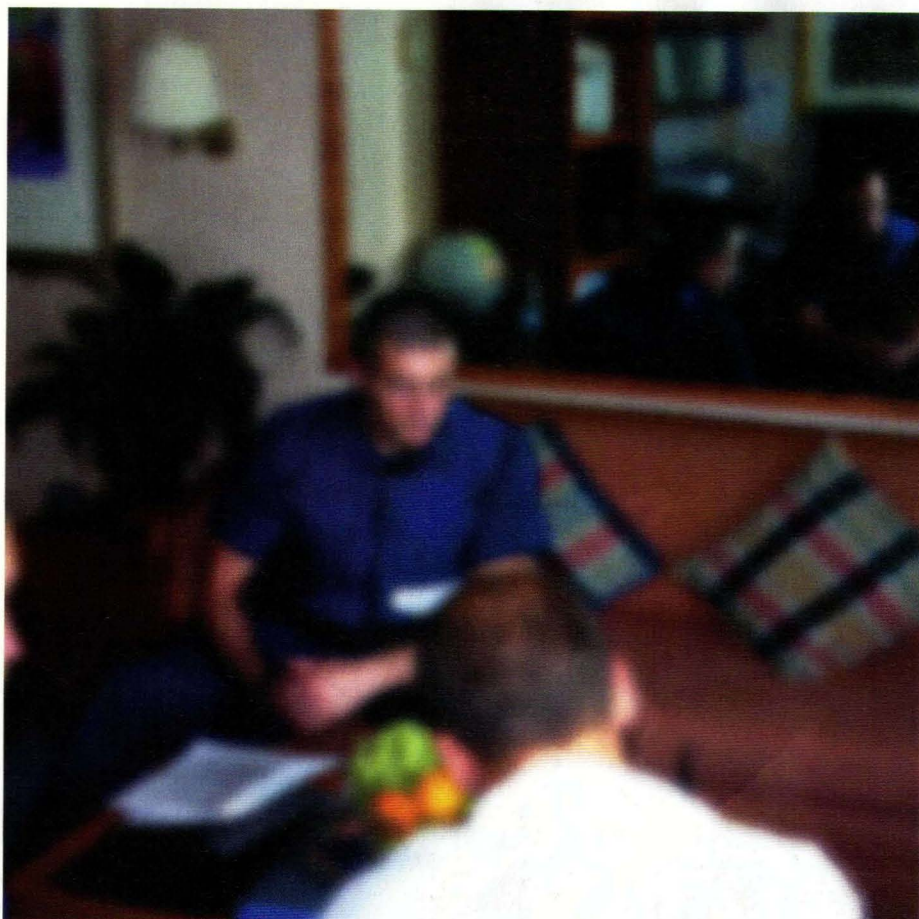
On 31 January 2001, Zakariaou's Rome apartment was burgled. At the time he told journalists: "I don't know if the theft in my apartment has anything to do with the infraction at the embassy [Niger's Vatican embassy had also just been broken into] and therefore the mysteries behind the construction of this false uranium dossier. I would like to know. But frankly, I don't think so. I think it was only a coincidence. At that time there had been several thefts in apartments in my neighbourhood..."



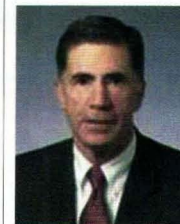
Elisabetta Burba passed documents to US Embassy officials in Rome

**Overleaf - US analyst warned Washington that it was impossible to transport uranium ore from Niger to Iraq -**





Laurence Silberman



Charles Robb

commission, and the president acted on their broad recommendations to reform our intelligence apparatus," said Frederick Jones, a spokesman for the National Security Council.

The assessment by the State Department's intelligence unit mirrored other investigative programmes, but as yet, its report is the only one made available to the public. It is known the CIA privately doubted the authenticity of the Niger Documents, though it seems unlikely its 'estimate of the situation' will be released.

The State Department's review looked at the political, economic and logistical factors in the "proposed" purchase, and

# SECRET INTELLIGENCE ASSESSMENT DOUBT

**A** State Department intelligence analyst examined information on Iraq's attempt to purchase yellowcake, a processed uranium ore from Niger, and concluded that it was "unlikely."

Without questioning the reliability of the intelligence, the analyst doubted the feasibility of moving large quantities of the material across 1,000 miles to Iraq. The secret classified documents - voicing the analyst's concerns - were recently released following a Freedom of Information Act request by Judicial Watch, a conservative legal group. The memo, dated 4 March 2002, was distributed at senior levels by the office of Secretary of State Colin L. Powell and by the Defense Intelligence Agency. It was also supplied to the US Embassy in London.

The documents state that because of economic, diplomatic and logistical obstacles, it was unlikely Saddam would mount such an operation. One problem cited in the assessment is that it would have required either country to use "25 hard-to-conceal 10-ton tractor-trailers." At least one international border would also

~~(S/NF)~~ NIGER: SALE OF URANIUM TO IRAQ IS UNLIKELY  
32. ~~(S/NF)~~ NIGER PROBABLY IS NOT PLANNING TO SELL URANIUM  
TO IRAQ, IN PART BECAUSE FRANCE CONTROLS THE URANIUM  
INDUSTRY IN NIGER AND WOULD TAKE ACTION TO BLOCK A SALE

have been crossed as the consignment wended its way to Iraq.

In 2003, President Bush announced that Saddam Hussein had sought significant quantities of uranium from the African nation; this was followed by an admission that the intelligence on the transaction was faulty.

Analysts have previously raised questions about the State Department's concerns over the Niger-Iraq affair, but the release of these documents provides evidence that US intelligence was "split" over Saddam's "chase" for a nuclear bomb.

Asked to discuss the implications of the assessment, The White House declined to discuss details of the declassified memo. "This matter was examined fully by the bipartisan Silberman-Robb

beyond the obvious. Other assessments are known to have supported the view that Saddam would eventually like to complete a nuclear warhead, though even the CIA believe that the former dictator had abandoned his plans.



President Mamadou Tandja

Following the analyst's work, the State Department concluded that Niger was "probably not planning to sell uranium to Iraq," possibly because France controlled the uranium industry in the country and could block such a sale. As for intelligence indicating Niger's president, Mamadou Tandja, could have already set the wheels in motion with Iraq in 2000,





Uranium ore being transported by road. US analyst believed it would be impossible to move the material 1,000 miles by road without being seen

the review felt that Mr Tandja would not jeopardise his country's foreign aid from the United States and other allies.

The State Department questioned Niger's ability to deliver 500 tons of uranium even if the sale were attempted. "Moving such a quantity secretly over such a distance would be very difficult, particularly because the French would be indisposed to approve or cloak this arrangement."

# URANIUM SALE



Colin Powell with President Bush

~~SECRET~~

~~NOFORN~~

UNCLASSIFIED

PRESIDENT TANDJA NOR KEY OFFICIALS OF HIS GOVERNMENT, WHO UNDERSTAND THE VALUE OF GOOD RELATIONS WITH THE U.S. AND OTHER AID DONORS, WOULD RISK JEOPARDIZING THEM BY SELLING URANIUM TO IRAQ. IN ADDITION, THE SALE WOULD VIOLATE UN SECURITY COUNCIL RESOLUTION 687.

33. ~~(S)~~ FRANCE, WHICH USES NUCLEAR POWER TO PRODUCE ABOUT 80 PERCENT OF ITS ELECTRICITY, OBTAINS AROUND 40 PERCENT OF ITS URANIUM FROM TWO MINES AT ARLIT, DEEP IN THE SAHARA IN NORTHERN NIGER -- THE ONLY OPERATING URANIUM MINES IN THE COUNTRY. FRANCE AND NIGER JOINTLY OWN THE MINES; JAPAN AND SPAIN HAVE A MINORITY INTEREST IN ONE OF THEM. FRANCE UNEQUIVOCALLY CONTROLS THE OVERALL OPERATION; THERE ARE FRENCH MANAGERS AND ENGINEERS AT EVERY POINT IN THE MINING, MILLING, AND TRANSPORTATION PROCESS.

34. ~~(S/NF)~~ A CORRUPT FORMER PRESIDENT MAY HAVE NEGOTIATED WITH IRAQ. [

] AT THAT TIME NIGER WAS RULED BY PRESIDENT BARE MAINASSARA, AN UNSOPHISTICATED AND VENAL

B1  
B3

~~SECRET~~

~~NOFORN~~

UNCLASSIFIED

URANIUM. THOUGH THE ALLEGED AGREEMENT WITH IRAQ IS NOT SPECIFIC, IT APPARENTLY CALLS FOR THE 500 TONS TO BE DELIVERED [ IN ONE YEAR. THIS WOULD MEAN THAT [ 25 HARD-TO-CONCEAL 10-TON TRACTOR-TRAILERS WOULD BE USED TO TRANSPORT THE OFF-THE-BOOKS URANIUM. BECAUSE NIGER IS LANDLOCKED THE CONVOY WOULD HAVE TO CROSS AT LEAST ONE INTERNATIONAL BORDER AND TRAVEL AT LEAST 1,000 MILES TO REACH THE SEA. MOVING SUCH A QUANTITY SECRETLY OVER SUCH A DISTANCE WOULD BE VERY DIFFICULT, PARTICULARLY BECAUSE THE FRENCH WOULD BE INDISPOSED TO APPROVE OR CLOAK THIS ARRANGEMENT.

POWELL  
ADMIN

B1  
B1

The analyst's report was distributed to senior figures in the office of former Secretary of State Colin Powell and the Central Intelligence Agency. Together with the DIA, all these agencies doubted Iraq was seeking uranium ore from Niger



Chris Farrell, the director of investigations at Judicial Watch and a former military intelligence officer, said: "The State Department's analysis is very strong, well-thought-out argument that looks at the whole playing field in Niger, and it makes a compelling case for why the uranium sale was so unlikely."

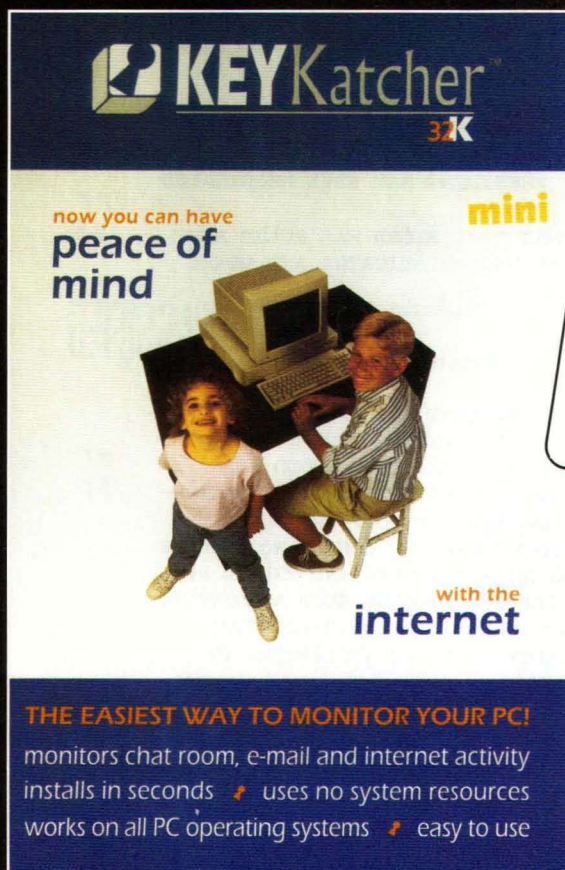
The question arises therefore, was President Bush advised on the assessment. An official responding to that question answered: "The White House is not an intelligence-gathering operation. The president based his remarks in the State of the Union address on the intelligence that was presented to him by the intelligence community and cleared by the intelligence community. The president has said the intelligence was wrong, and we have reorganised our intelligence agencies so we can do better in the future."



# AVAILABLE FROM EYE SPY

Not only is this well constructed item a valuable security tool, it is ideal for parents to protect children from the ever-present dangers on the internet. You will see conversations they are having and know which web sites they are visiting. E-mail and chat room activities are captured for you to see. Although there is no "off-the-shelf" solution for effective parenting, the KEYKATCHER will be your eyes when you're away. It will provide you with the information you need to protect and communicate with your family.

OF COURSE IT IS MORE WIDELY USED AS A COVERT ESPIONAGE DEVICE



**KEYKatcher**  
32K

now you can have  
**peace of mind**

**mini**

with the  
**internet**

**THE EASIEST WAY TO MONITOR YOUR PC!**  
monitors chat room, e-mail and internet activity  
installs in seconds • uses no system resources  
works on all PC operating systems • easy to use



- Search capability
- Memory remains intact even when unplugged or during power loss
- No software to install
- Virtually undetectable

#### System Requirements

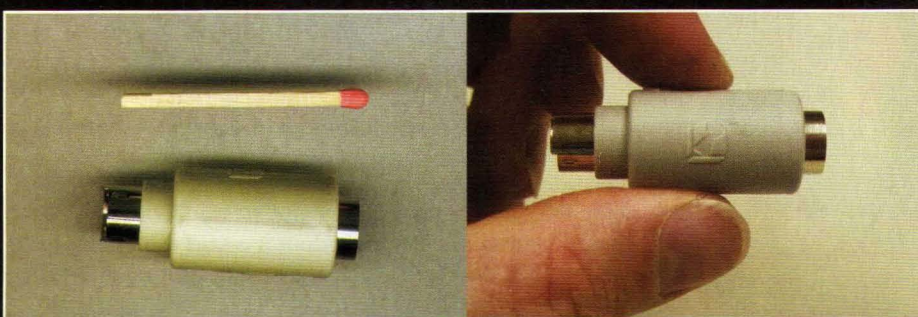
IBM PC compatible computer  
(Windows 98, 95, NT Linux)

PS/2 keyboard connector

**PORTABLE:** The Keykatcher is a hardware only monitoring device. Unlike software, it can be easily moved from computer to computer. You can record on one computer, and read the memory contents on another 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

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

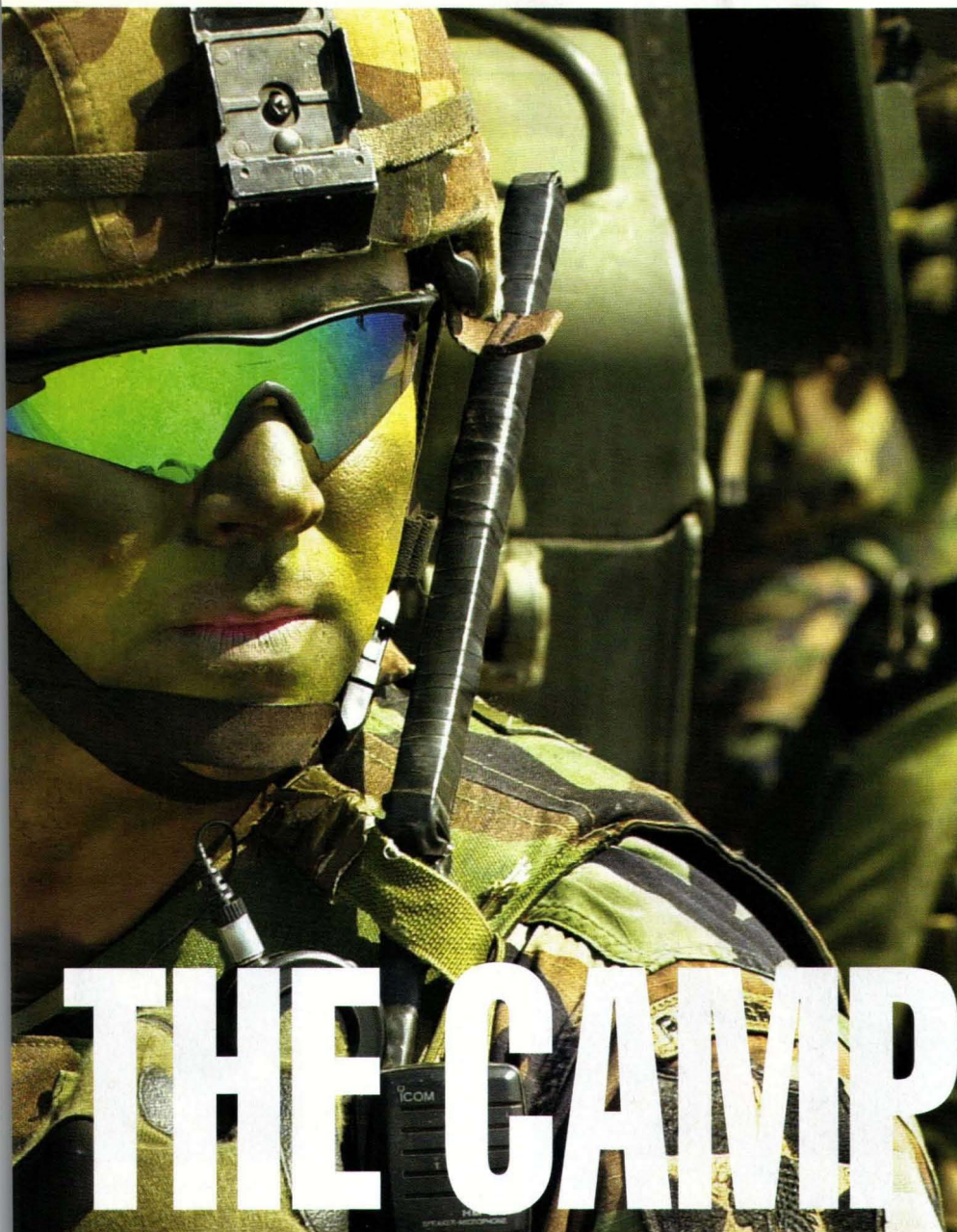


Russian  
Ambassador  
Provided  
Saddam with  
2003 Bogus  
US Battle  
Plan...  
or did he?

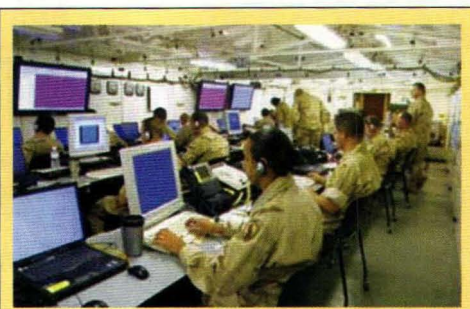
# SPY IN OR AGE

According to information contained in two captured Iraqi intelligence documents released by the Pentagon in March, it appears someone from US Central Command headquarters, which is sited at Camp As Saliyah just outside Doha, the capital of Qatar, tipped-off a Russian agent who in turn forwarded the battle plans to a senior Russian diplomat in Baghdad. Russia's ambassador then allegedly forwarded the information to Saddam's military commanders.





# T APRIL FOOL?



One document, referenced as **CMPC-2003-001950** is a handwritten account of a meeting with the Russian ambassador that details his description of the composition, size, location and type of US military forces arrayed in the Gulf and Jordan. The document includes the exact numbers of tanks, armoured vehicles, different types of aircraft, missiles, helicopters, aircraft carriers, and other forces, and also includes their exact locations. The ambassador also described the positions of two Special Forces units.

Document **CMPC-2004-001117** is a typed account, signed by Deputy Foreign Minister Hammam Abdel Khaleq, that states that the Russian ambassador has told the Iraqis that the United States was planning to deploy its force into Iraq from Basra in the South and up the Euphrates, and would avoid entering major cities on the way to Baghdad, which is, in fact what happened. The documents also state "Americans are also planning on taking control of the oil fields in Kirkuk". The information was obtained by the Russians from "sources at US Central Command in Doha, Qatar" (above), according to the document.

US Joint Forces Command in Norfolk, Virginia, which has analysed tens of thousands of captured Iraqi documents. The report also contains interviews with senior Iraqi political and military leaders.

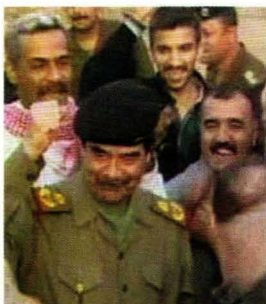
The two released documents described how Russian officials "drawing on their sources inside the American Central Command in Doha" gave Baghdad intelligence on US troop movements and war plans to Saddam Hussein as Coalition forces attacked in March and April 2003.

There is the possibility that the documents are not authentic, a reference to the source of the material. "It's important to remember that the information came from an Iraqi intelligence report. Central Command does not vouch for the documents accuracy or authenticity," an e-mailed response to a question stated.

However, these views contrast with conclusions reached in the study: "The Iraqi documents are authentic," said Retired Lt. Col. Kevin M. Woods, the project's director. "There is no reason to doubt the Iraqi documents," he said. Asked about possible breaches in security, Woods said: "I don't have any other knowledge of that topic." But he did find

Intelligence and military officials have thus far refused to launch an investigation, though the CIA and other agencies are puzzled how the Russians acquired the highly secret information.

The reasons behind the decision not to investigate are unclear, but speculation is rife that the material contained a great deal of disinformation and that the entire affair may have been a careful military intelligence ruse.



Central Command, commenting on media speculation that it had released disinformation deliberately said: "such external sources of information were only one of the fog-generators obscuring the minds of Iraq's senior leadership."

The information is contained in a classified 210-page report, titled 'Iraqi Perspectives Project', of which small portions have been made public. It was assembled by



# ANALYSING THE INTELLIGENCE

The Iraqi documents reveal intelligence (some of which was inaccurate) reportedly provided by Russia on the impending invasion of Iraq

- **US manoeuvres in southern Iraq from Kuwait is a diversion.**

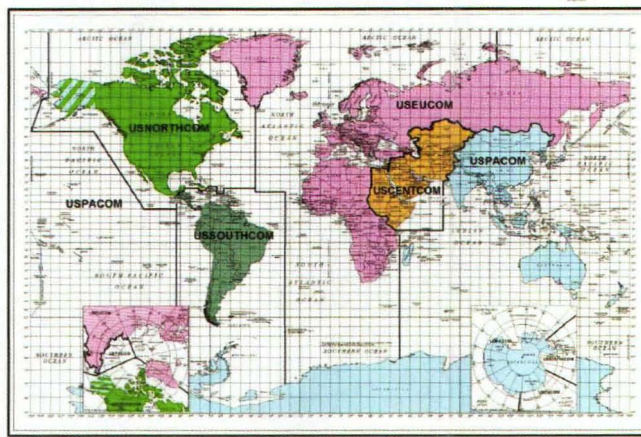
[The problem for Iraq's Army planners was that the intelligence was wrong - Primary Coalition forces actually took this route. Special Forces supported the thrust by entering Iraq via Jordan and flying paratroopers into northern Iraq]

- **The US ground assault on Baghdad would not begin until the Army's 4th Infantry Division was in place - probably around 15 April.** [The intelligence was flawed, but only because the 4th Infantry Division was not even in

Iraq. Turkey had objected to Coalition forces using its sovereign soil to launch a northern attack on Iraq. The force had to be re-routed. Unfortunately, the information was a bonus for US planners and an inadvertent piece of disinformation that may have confused Iraq's military. However, such was the speed of the advance, the actual ground assault began 7 April]

- **The area around the city of Karbala would be used to move US ground forces towards Baghdad from the southwest.** [The intelligence was accurate.

THE WORLD WITH COMMANDERS' AREAS OF RESPONSIBILITY



After the 3rd Infantry Division crossed the River Euphrates outside Karbala, the road was clear through to Baghdad]

- **Coalition forces had no intention of taking major cities and towns in southern Iraq. They**

**would simply bypass them.**

[Military analysts were surprised at the speed of the Coalition's thrust towards Baghdad. Besides little Iraqi resistance, this was due to the fact that most centres of populace were simply bypassed]

COURTESY: US ARMY



US Central Command Headquarters at Sayliyah military base in Qatar

A Central Command official said the organisation "takes all matters of operational security seriously." When asked if an official investigation would be forthcoming, he said that the command was "not probing" the affair.

"Centcom has not opened an investigation at this time," said Captain Christopher Augustine, a spokesman for the Florida-based command, which controls military operations in the Middle East and other areas.



Russia has denied its ambassador passed on intelligence to Saddam Hussein

## AGENT APRIL FOOL

it "surprising" [if] the Russians had "passed intelligence to Saddam."

Some military officials are concerned that if the documents are genuine, the leak almost certainly occurred from inside Central Command. Secretary of State Condoleezza Rice said that the Bush administration would take "a real hard look at the documents and then raise it with the Russian government." This prompted an immediate response from Moscow. Russia's intelligence service (FSB) issued a statement saying the allegations in the documents are "baseless

accusations" and "fabrications." Moscow has since denied that Russian officials gave Hussein information on the US military operations in Iraq. However, Pavel Felgenhauer, a respected independent Moscow-based military analyst, revealed that a Russian military intelligence unit, known by its abbreviation GRU, was active in Iraq at the time of the invasion.

The Russian ambassador in Baghdad at the time was Vladimir Teterenko. He was cited by the Volcker Commission as having received \$1.5 million worth of allocations from Saddam in the Oil-for-Food scandal.

A Central Command spokesman, said no one in his office knew of the existence of the Iraqi documents before the Iraqi Perspectives Project study release, and that it was "highly possible" the military released them without prior vetting by Central Command.

### Agent April Fool

While some US politicians and intelligence officials believe a genuine leak did occur at Centcom, the truth is far more interesting. Some eighteen months ago, Eye Spy learned that Centcom had created a highly secret 'deception unit' whose agents were charged with spreading disinformation to various persons and





Army General Tommy Franks, commander of US Central Command, speaks with reporters outside a hotel in Abu Dhabi, United Arab Emirates

groups that would confuse Saddam. Indeed, it is likely the Russian diplomat was given incorrect US invasion plans by an undercover officer codenamed April Fool. The identity of the US military agent remains a closely guarded secret, but he had already managed to deceive a senior Iraqi diplomat, by providing the same bogus battle plans that showed the invasion of Iraq would come from the north.

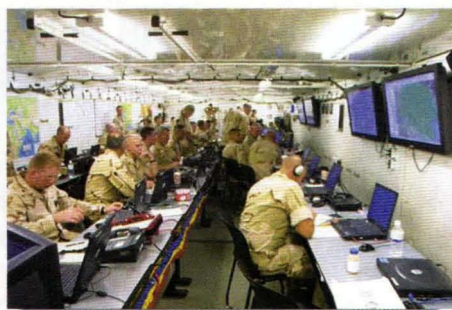


deliver tanks and Bradley fighting vehicles to join them.

"If the deception succeeded, Saddam would keep the better part of 13 divisions north of Baghdad to defend against the 4th Infantry until it was too late to use them to counter the main Coalition attack coming out of Kuwait.

"I knew what our reconnaissance imagery told us," said Franks. "Despite our sizable build-

US Commander General Tommy Franks said that by the time Saddam had realised what was happening, it was already too late. "Because of the sensitivity of the deception, only a few people in the US Government were aware of it," said Franks.



April Fool's reports went directly to Baghdad for action. The US agent sold the Iraqi 'top secret' invasion plans complete with codes and a series of seemingly authentic manoeuvres. Unbeknownst to Baghdad, they had been created by Centcom.

General Franks said: "The storyline we sold them went as follows: the Coalition was planning to build up only a portion of its ground force in Kuwait, while preparing a major airborne assault into northern Iraq from above Tikrit to the oil fields around the city of Kirkuk. Helicopter-borne air assault forces would then reinforce the paratroopers. Then, once several airstrips were secured, C-17 transports would

up of forces in Kuwait to the south, Saddam's Republican Guard and regular army divisions had not moved significantly from their northerly positions - no doubt waiting for an assault that would never come."

(See *Eye Spy* 28 for full story on Agent April Fool)



# EYE SPY

# SUBSCRIBE

INTELLIGENCE MAGAZINE







# EYE SPY TRADE BOOKS 2000

## INTELLIGENCE MAGAZINE

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

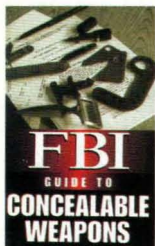
For detailed information on these and many more titles go to [www.eyespy.com](http://www.eyespy.com)

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

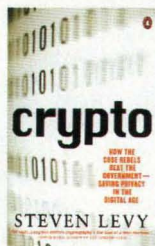
[www.eyespy.com](http://www.eyespy.com)  
FOR OUR FULL SELECTION  
OF TRADE BOOKS



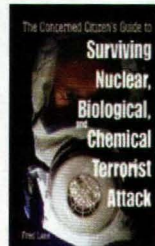
Use order form on page 82 - or go to [www.eyespy.com](http://www.eyespy.com) or telephone direct



**FBI GUIDE TO CONCEALABLE WEAPONS**  
Packed with photos. Softback 86pp  
E9966 \$18.00 \$25.00



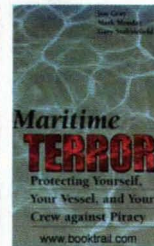
**CRYPTO** Code rebels. Humble the hackers and spooks. Essential. Paperback 352pp  
E9903 \$10.00 \$20.00



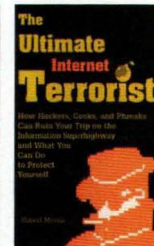
**CITIZEN'S GUIDE** Surviving nuclear, biological, chemical attacks. Softback 80pp  
E8866 \$17.00 \$22.50



**SECRET SOFTWARE** Data, forensics, crime investigation. Softback 128pp  
E861 \$20.00 \$38.00



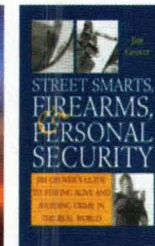
**MARITIME TERROR** Protection against piracy. Softback 72pp  
E869 \$14.50 \$30.50



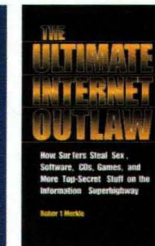
**ULTIMATE INTERNET TERRORIST** The dangers revealed. Softback 152pp  
E1041 \$18.00 \$36.00



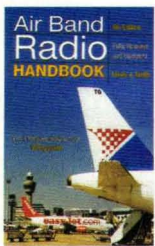
**UBERHACKER II MORE WAYS TO BREAK INTO A COMPUTER** Softback 370pp  
E1039 \$39.95 \$68.00



**STREET SMARTS, FIREARMS, AND PERSONAL SECURITY** Guide to Staying Alive. Softback 280pp  
E1111 \$28.00 \$45.00



**ULTIMATE INTERNET OUTLAW** Softback 96pp  
E1040 \$15.00 \$29.00



**AIR BAND RADIO HANDBOOK 2005** For the enthusiast and professional alike. Softback 208pp  
E9971 \$14.99 \$30.00



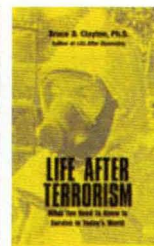
**US ARMY SPECIAL FORCES MEDICAL HANDBOOK** Softback 608pp  
E1094 \$30.50 \$35.00



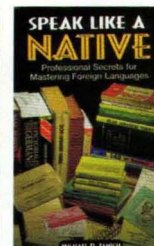
**RAGNAR'S URBAN SURVIVAL** Staying alive in the city. Softback 200pp  
E1097 \$20.00 \$25.00



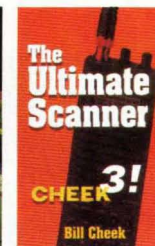
**SPYING A RING OF SPIES** Spy craft and black operations in the real world of espionage. Softback 216pp  
E860 \$25.00 \$48.00



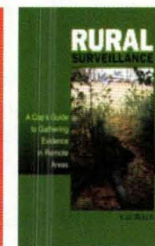
**LIFE AFTER TERRORISM** What you need to know to survive today. Softback 192pp  
E868 \$21.50 \$40.00



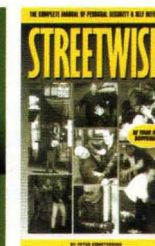
**SPEAK LIKE A NATIVE** Professional secrets for mastering foreign languages. Softback 192pp  
E961 \$20.00 \$30.00



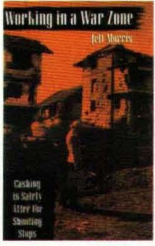
**THE ULTIMATE SCANNER** The complete guide to scanning. Large Softback 242pp  
E963 \$34.99 \$48.00



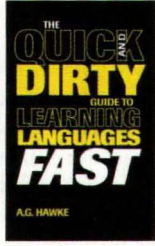
**RURAL SURVEILLANCE** Police guide to gathering evidence in remote areas. Softback 128pp  
E881 \$22.00 \$40.00



**STREETWISE** The complete manual of personal security and self-defence. 314pp  
E808 \$25.00 \$40.00



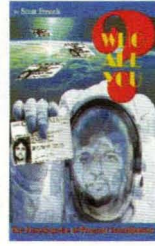
**WORKING IN A WAR ZONE** Cashing in safely after the shooting stops. Softback 184pp  
E875 \$17.50 \$34.00



**QUICK AND DIRTY GUIDE TO LEARNING LANGUAGES FAST** Softback 176pp  
E1018 \$20.00 \$37.99



**ADVANCED SURVEILLANCE** Complete Manual of Surveillance Training. Softback 400pp  
E5712 \$24.99 \$40.00



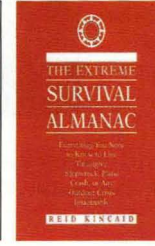
**WHO ARE YOU?** The encyclopedia of personal identification. Softback 352pp  
E1006 \$26.95 \$50.00



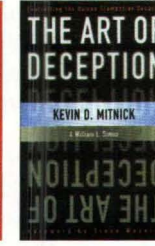
**SECRETS OF STREET SURVIVAL** Staying alive in a civilian warzone. Softback 400pp  
E809 \$29.99 \$50.00



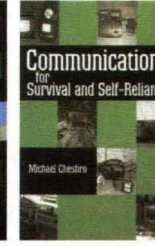
**DON'T BUG ME** The Latest High-Tech Spy Methods. Softback 152pp  
E1005 \$22.95 \$45.00



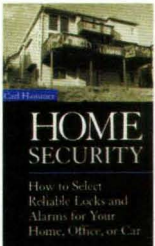
**EXTREME SURVIVAL ALMANAC** Everything you need to know. Softback 480pp  
E1093 \$50.00 \$56.00



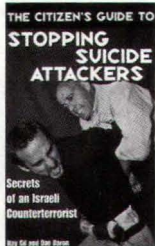
**THE ART OF DECEPTION** Controlling the human element of security. Softback 352pp  
E803 \$12.99 \$23.00



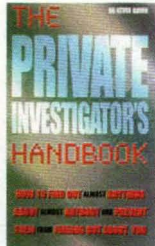
**COMMUNICATIONS FOR SURVIVAL AND SELF-RELIANCE** Softback 216pp  
E1096 \$30.00 \$35.00



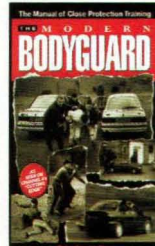
**HOME SECURITY** How to select locks and alarms for your home/business. Softback 128pp  
E988 \$22.99 \$32.00



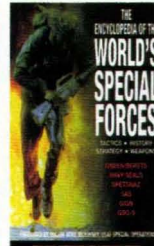
**STOPPING SUICIDE ATTACKERS** Secrets of an Israeli counterterrorist. Softback 192pp  
E865 \$20.00 \$38.50



**PRIVATE INVESTIGATOR'S HANDBOOK** How to find out anything on anybody. 192pp  
E813 9.99 \$25.00



**MODERN BODYGUARD** The manual of close protection and training. Softback 332pp  
E607 \$25.00 \$40.00



**WORLD'S SPECIAL FORCES** Encyclopedia of special forces, air, sea, land. Hardback 255pp  
E886 \$28.00 \$55.00



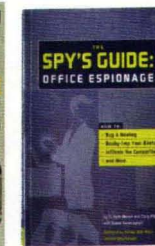
**CHECK IT OUT** How to find out practically anything. Softback 160pp  
E1074 \$19.00 \$28.00



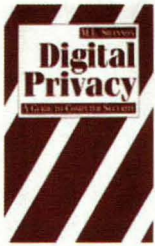
**PRACTICAL MARTIAL ARTS FOR SPECIAL FORCES** How to use your hands. Softcover, 112pp  
E1091 \$18.00 \$24.00



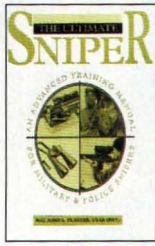
**DO IT YOURSELF MEDICINE** How to find and use the most effective drugs. Softback 128pp  
E1095 \$20.00 \$23.00



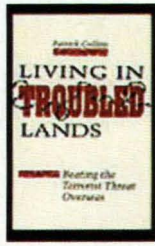
**THE SPY'S GUIDE: OFFICE ESPIONAGE** Professional tips. Softback 170pp  
E722 \$12.00 \$20.00



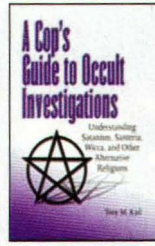
**DIGITAL PRIVACY** A guide to computer security. Essential tips. Softback  
E1003 \$25.00 \$50.00



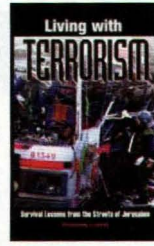
**THE ULTIMATE SNIPER** Advanced training for military and police. Huge Softback 543pp  
E965 \$50.00 \$70.00



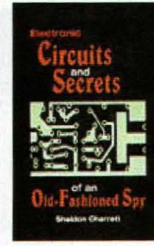
**LIVING IN TROUBLED LANDS** Beating the Terrorist Threat Overseas. Softcover 192pp  
E1113 \$21.00 \$35.00



**COP'S GUIDE TO OCCULT INVESTIGATIONS** A police must. Softback 184pp  
E1043 \$25.00 \$29.00



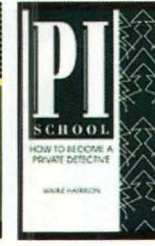
**LIVING WITH TERRORISM** Survival Lessons From the Streets of Jerusalem. Softback  
E1116 \$19.00 \$30.00



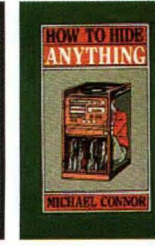
**ELECTRONIC CIRCUITS AND SECRETS** old-fashioned spy - bugs and more. Softback 128pp  
E908 \$22.99 \$40.00



**SCANNER MODIFICATIONS AND ANTENNAS** Modifying equipment. Softback 176pp  
E910 \$18.00 \$35.00

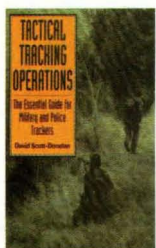


**PI SCHOOL: HOW TO BE A PRIVATE INVESTIGATOR** Softback 112pp  
E1072 \$19.00 \$25.00



**HOW TO HIDE ANYTHING** Learn how to construct dozens of hiding places. Softback 120pp  
E1117 \$16.00 \$26.00

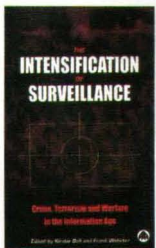




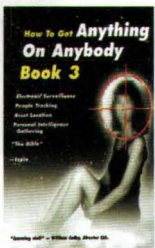
**TACTICAL TRACKING OPERATIONS**  
The Essential Guide for Military and Police Trackers  
Softback 170pp  
£827 \$38.00 \$60.00



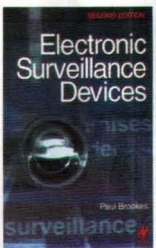
**INVISIBLE ADVANTAGE**  
Chillie suit construction made simple  
Softback 80pp  
£914 \$13.99 \$25.00



**THE INTENSIFICATION OF SURVEILLANCE**  
Crime, terrorism and warfare  
Softback 176pp  
£825 \$25.00 \$45.00



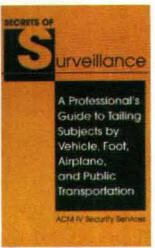
**How to Get Anything on Anybody Book 3**  
Special Security Work  
Massive Softback  
£737 \$65.00 \$109.00



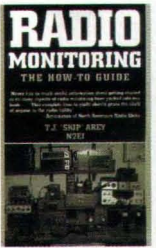
**ELECTRONIC SURVEILLANCE DEVICES**  
Micro-phones, transmitters etc.  
Softback 160pp  
£807 \$24.99 \$45.00



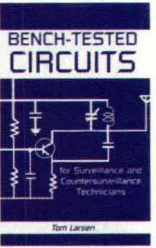
**RECOGNISING BIO ATTACKS** Anthrax, smallpox, nerve gas, radiation  
Softback 112pp  
£870 \$17.00 \$23.50



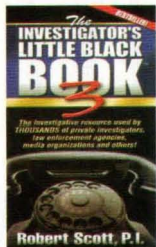
**SECRETS OF SURVEILLANCE**  
Professional guide to tailing subjects  
Softback 248pp  
£814 \$29.99 \$50.00



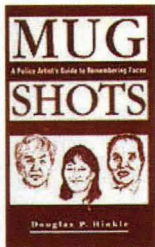
**RADIO MONITORING**  
The 'know how guide' packed with tips  
Softback 176pp  
£964 \$25.00 \$35.00



**BENCH-TESTED CIRCUITS**  
For countersurveillance technicians  
Softback 128pp  
£824 \$15.00 \$32.00



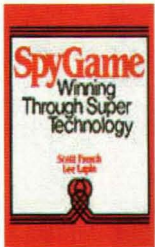
**INVESTIGATOR'S LITTLE BLACK BOOK 3**  
Major US-based resource guide  
Softback 504pp  
£806 \$19.99 \$35.00



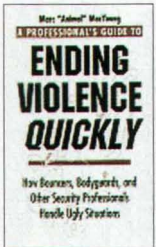
**MUG SHOTS**  
A police detective guide to remembering faces  
Softback 128pp  
£880 \$20.00 \$38.00



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



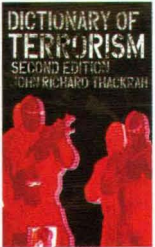
**SPY GAME** Winning through super technology  
Huge Softback 520pp  
£862 \$35.00 \$60.00



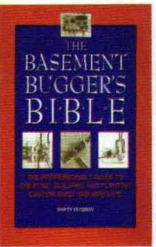
**ENDING VIOLENCE QUICKLY** Avoid injuries and law suits - professional guide  
Softback 256pp  
£894 \$21.99 \$40.00



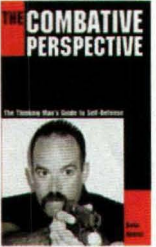
**EXECUTIVE PROTECTION** A professional's guide to bodyguarding  
Softback 112pp  
£872 \$15.50 \$31.00



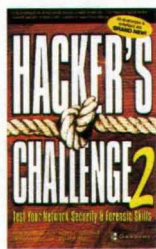
**DICTIONARY OF TERRORISM** Every group, individual listed. Essential  
Softback 448pp  
£975 \$25.00 \$48.00



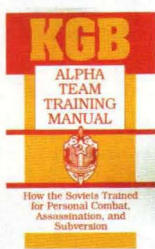
**THE BASEMENT BUGGER'S BIBLE** Everything you need to know about bugs  
Softback 312pp  
£947 \$34.99 \$60.00



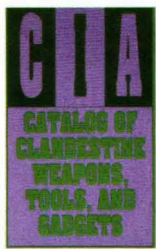
**COMBAT PERSPECTIVES** The thinking man's guide to self-defence  
Softback 112pp  
£884 \$17.50 \$34.00



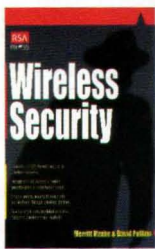
**HACKER'S CHALLENGE 2** Test your security and forensic network skills  
Large Softback 320pp  
£982 \$25.00 \$48.00



**KGB ALPHA TEAM TRAINING MANUAL** How the Soviets Trained for Personal Combat, Assassination, and Subversion  
Softback 320pp  
£808 \$24.99 \$45.00



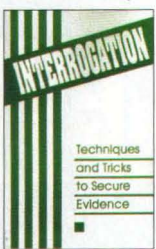
**CIA CATALOG** Clandestine weapons, tools and gadgets  
Softback 128pp  
£944 \$18.00 \$28.00



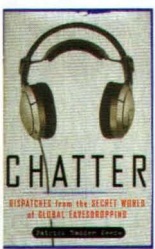
**WIRELESS SECURITY** Professional tips to secure your wireless network  
Softback 300pp  
£980 \$25.00 \$49.99



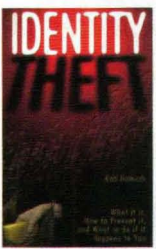
**HIDING IN PLAIN SIGHT** Superb guide to steganography plus CD ROM  
Softback 335pp  
£802 \$27.00 \$45.00



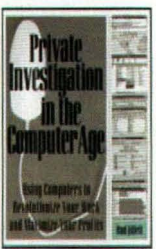
**INTERROGATION** RCMP guide, techniques and tricks to secure evidence  
Softback 88pp  
£811 \$19.50 \$38.00



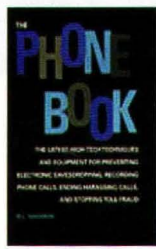
**CHATTER** Conversations from the secret world of eavesdropping  
Hardback 300pp  
£950 \$25.00 \$35.00



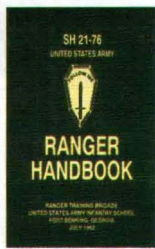
**IDENTITY THEFT** Secrets of countering identity theft and protecting yourself  
Softback 241pp  
£950 \$12.99 \$25.00



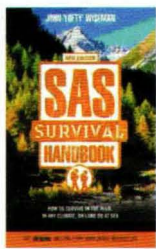
**PRIVATE INVESTIGATION IN THE COMPUTER AGE** Using computers to revolutionize your work and the computer police  
Softback 176pp  
£859 \$25.50 \$50.00



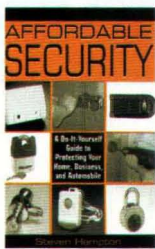
**THE PHONE BOOK** Stop eavesdroppers, telephone bugs, phone call fraud and more  
Softback 280pp  
£858 \$30.00 \$60.00



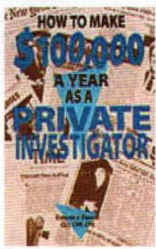
**RANGER HANDBOOK** US Army Ranger. Rare old manual  
Softback 448pp  
£810 \$26.00 \$48.00



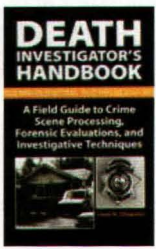
**SAS SURVIVAL HANDBOOK** Survive in any climate, land or sea  
Softback 576pp  
£830 \$24.00 \$45.00



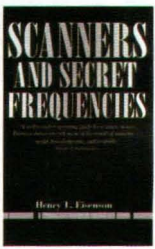
**AFFORDABLE SECURITY** Survive in any climate, land or sea  
Huge Softback 302pp  
£830 \$24.00 \$45.00



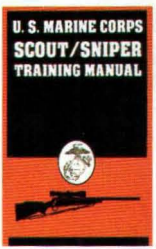
**HOW TO MAKE \$100,000 A YEAR AS A PRIVATE INVESTIGATOR**  
Softback 128pp  
£857 \$21.50 \$40.00



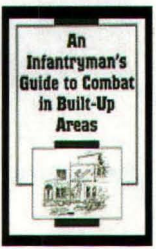
**DEATH INVESTIGATORS HANDBOOK** Field guide to crime scene forensics  
Massive Hardback 888pp  
£879 \$75.00 \$100.00



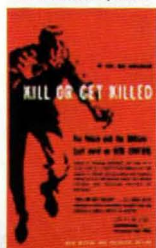
**SCANNERS AND SECRET FREQUENCIES** All you need to know  
Softback 314pp  
£967 \$25.00 \$38.00



**U.S. MARINE CORPS SCOUT/SNIPER TRAINING MANUAL** Marine Corps  
Softback 576pp  
£959 \$29.99 \$40.00



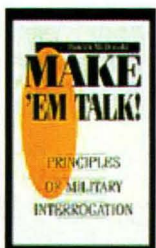
**COMBAT IN URBAN AREAS** Ground operations in urban settings  
Softback 312pp  
£888 \$29.99 \$58.00



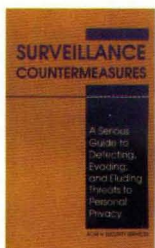
**KILL OR GET KILLED** The most selling book on close combat in history  
Softback 420pp  
£889 \$45.99 \$80.00



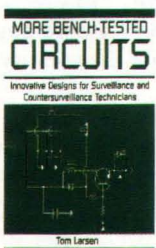
**THE WHOLE SPY CATALOG** Everything you need to know about espionage  
Softback 448pp  
£886 \$35.00 \$55.00



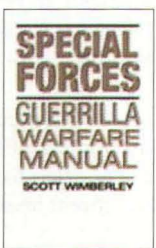
**MAKE 'EM TALK!** Principles of military interrogation. Professional guide  
Softback 80pp  
£890 \$17.99 \$35.00



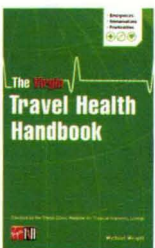
**SURVEILLANCE COUNTERMEASURES** Detecting, evading and enduring threats  
Softback 180pp  
£835 \$29.99 \$48.00



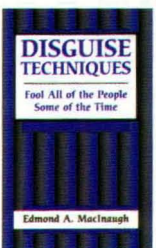
**MORE BENCH-TESTED CIRCUITS** Innovative designs for surveillance and countersurveillance technicians  
Softback 72pp  
£909 \$19.99 \$38.00



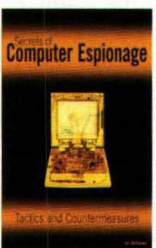
**SPECIAL FORCES GUERRILLA WARFARE MANUAL** Guerrilla warfare manual for successful operations  
Softback 248pp  
£912 \$22.99 \$42.00



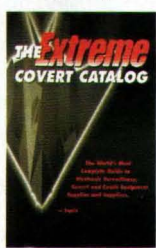
**VIRGIN TRAVEL HEALTH HANDBOOK - 2003** Business, professional or casual travel  
Softback 288pp  
£572 \$17.50 \$34.00



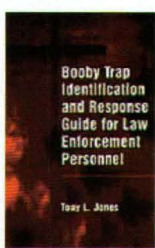
**DISGUISE TECHNIQUES** Fool all of the people some of the time  
Softback 82pp  
£962 \$18.00 \$28.00



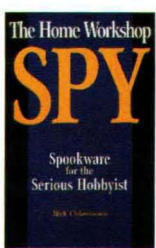
**SECRETS OF COMPUTER ESPIONAGE** Tactics and countermeasures  
Softback 240pp  
£831 \$29.99 \$48.00



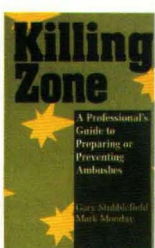
**THE EXTREME COVERT CATALOG - SPECIAL TRADE SECURITY WORK - IMPORTED**  
Massive Softback  
£738 \$50.00 \$60.00



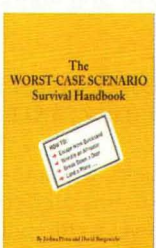
**BOOBY TRAP IDENTIFICATION** Response guide for law enforcement personnel  
Softback 80pp  
£876 \$20.00 \$38.00



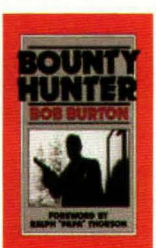
**HOME WORKSHOP SPY** Spookware for the serious hobbyist  
Softback 104pp  
£856 \$24.50 \$48.00



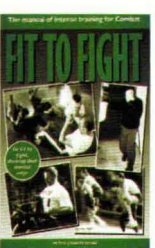
**KILLING ZONE** A professional's guide to preventing ambushes  
Softback 240pp  
£960 \$25.00 \$40.00



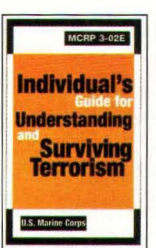
**WORST-CASE SCENARIO TRAVEL** Survival handbook  
Softback 192pp  
£805 \$12.00 \$24.00



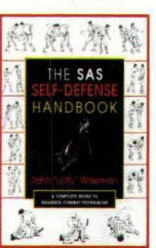
**BOUNTY HUNTER** Professional guide to the art of bounty hunting  
Softback 136pp  
£873 \$15.50 \$30.00



**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-DEFENCE HANDBOOK** Complete guide to unarmed combat  
Softback 240pp  
£831 \$29.99 \$48.00





# THREAT LEVEL ALERTS FOR UK

## WARNING

**T**here was confusion in the UK when the public learned that the government had actually lowered the threat level just four weeks before terrorists attacked London on 7 July 2005. For those charged with assessing the danger to Britain, it was a huge embarrassment. Now, a cross-party committee investigating the background to the bombings is expected to recommend an official public warning system that will be 'visual' in various forms - from computer adverts to newspaper inserts to billboards. The levels will almost certainly be shown on all government websites; council and city websites are expected to follow. Intelligence sources say it will be virtually identical to that introduced in 2002 in the United States following 9/11.

Currently UK threat levels are set by the Joint Terrorism Analysis Centre (JTAC). Just before the London attacks, the level was 'severe general'... then it was downgraded to 'substantial'. In the aftermath of the four bombs, it was raised to 'critical'. Amazingly, on the morning of 21 July, JTAC was preparing to lower the level again, when news started to appear on

the television that four more terrorists had tried to detonate explosives.

The JTAC system has various levels, with 'moderate' being the lowest and 'severe specific' which effectively means "expect an attack to occur." However, this sets levels for transport, public and official buildings, but not the country.

Patrick Mercer, Conservative spokesman on homeland security, says that the public are entitled to more openness. "Currently, the threat levels are deeply confusing."

Intelligence sources say JTAC lowered the threat level just before 7/7 because it was basing its decision on the "threat of overseas terrorists" and not "home-grown bombers."

### THE US HOMELAND SECURITY ADVISORY SYSTEM

In the United States, a colour-coded Threat Level System is used to communicate the threat level to the public so that protective measures can be implemented to reduce the likelihood or impact of an attack. The higher the Threat Condition,

the greater the risk of a terrorist attack. Risk includes both the probability of an attack occurring and its potential seriousness.

The terrorist threat level is elevated when specific information about a threat to a particular sector or geographic region is received. Threat Conditions may be assigned for the entire nation, or they

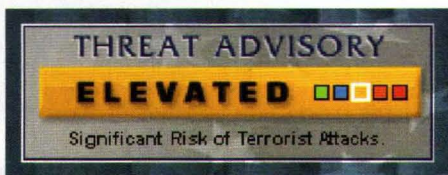






Below: The Home Office, London. Officials here will decide on the most appropriate threat level model

Left: Specialist New York City police officers are continually on a high alert. The city has a separate threat matrix, though uses the same colour-coded model as the rest of the USA



may be set for a particular geographic area or industrial sector.

In the United States, a colour-coded system is in place, though it has yet to rise to its highest level. When a rise in its status is made, the public are advised to be extra vigilant. Additional police and security services are placed on the streets and baggage searches and car checks are more prevalent. In New York City, the threat level has been operating at an Orange (High) threat ever since 9/11.

The exact criteria used to set the UK model will probably remain secret, though MI5, MI6, the Home and Foreign Office, plus JTAC are all expected to contribute. Currently, JTAC disseminates more than 50,000 items of intelligence every year.

Like New York City, London could be evaluated separately from the rest of the UK. This is one issue still to be decided by those developing the new threat level model

#### HOMELAND SECURITY ADVISORY SYSTEM DEFINITIONS

##### GREEN: LOW CONDITION

This condition is declared when there is a low risk of terrorist attacks

##### BLUE: GUARDED CONDITION

This condition is declared when there is a general risk of terrorist attacks

##### YELLOW: ELEVATED CONDITION

An Elevated Condition is declared when there is a significant risk of terrorist attacks

##### ORANGE: HEIGHTENED CONDITION

A High Condition is declared when there is a high risk of terrorist attacks

##### RED: SEVERE CONDITION

A Severe Condition reflects a severe risk of terrorist attacks

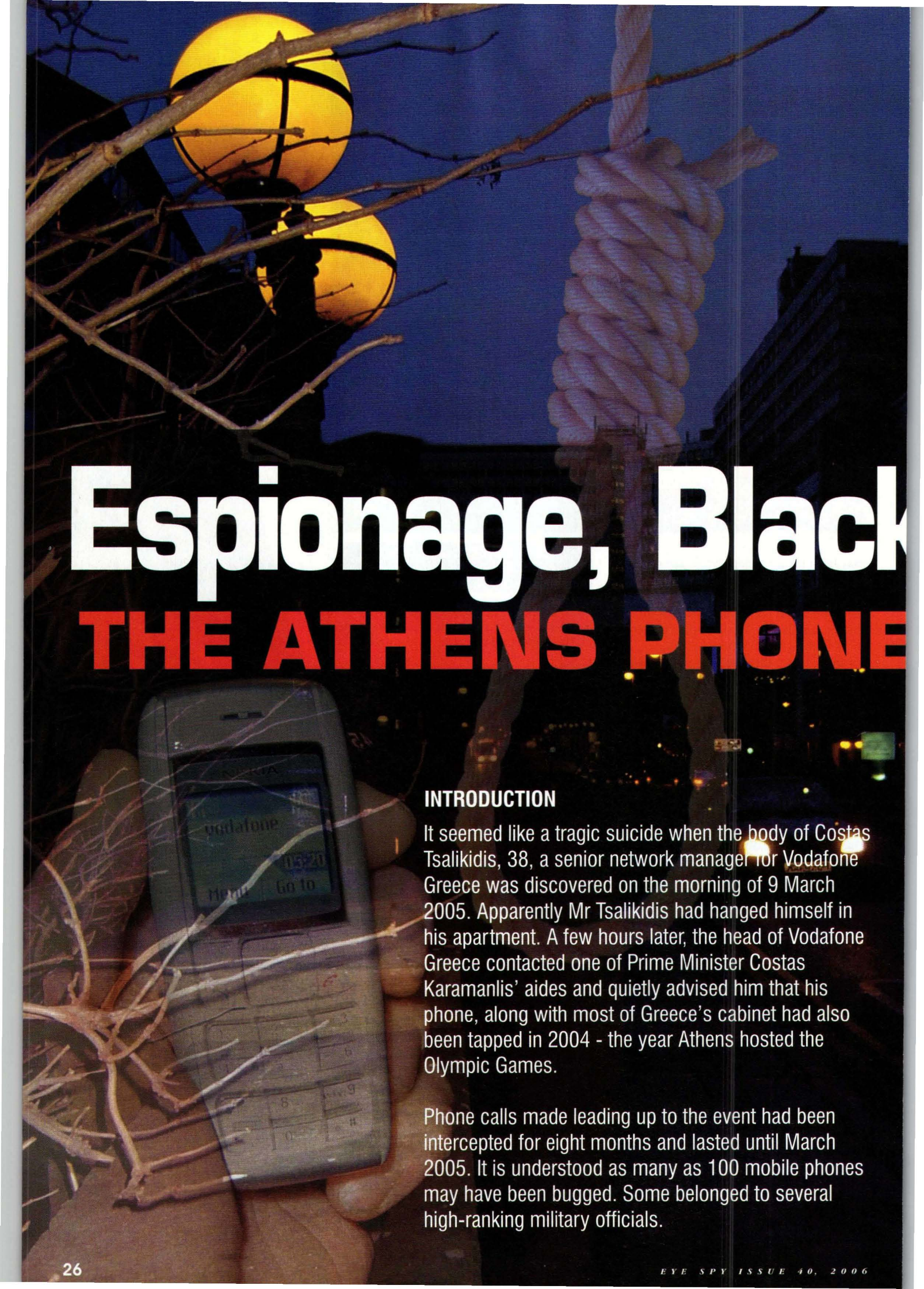
Each condition requires Federal agencies and security services to implement a number of measures. These can be found on most government web sites, or requesting a brochure from the police. However, in the case of 'Severe' - code Red, Homeland Security describes the following:

Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

1. Increasing or redirecting personnel to address critical emergency needs;
2. Assigning emergency response personnel and pre-positioning and mobilising specially trained teams or resources;
3. Monitoring, redirecting, or constraining transportation systems; and
4. Closing public and government facilities.







# Espionage, Black

## THE ATHENS PHONE

### INTRODUCTION

It seemed like a tragic suicide when the body of Costas Tsalikidis, 38, a senior network manager for Vodafone Greece was discovered on the morning of 9 March 2005. Apparently Mr Tsalikidis had hanged himself in his apartment. A few hours later, the head of Vodafone Greece contacted one of Prime Minister Costas Karamanlis' aides and quietly advised him that his phone, along with most of Greece's cabinet had also been tapped in 2004 - the year Athens hosted the Olympic Games.

Phone calls made leading up to the event had been intercepted for eight months and lasted until March 2005. It is understood as many as 100 mobile phones may have been bugged. Some belonged to several high-ranking military officials.



**F**ormer government spokesman Theodore Roussopoulos said: "The phones tapped included the prime minister's, those of cabinet members, one former minister, now in opposition, and others. The phone tapping was carried out by [an] unknown person or persons using high technology."

The Greek authorities launched an inquiry and established a parliamentary committee to investigate the espionage. Many people have been questioned, including senior officials from Vodafone and Ericsson. Intelligence officials are now focusing their attention on the

fallen on Costas Tsalikidis and the Central Intelligence Agency. For its part Vodafone issued a statement categorically denying any connection between the death of Tsalikidis and the phone tapping. "Any attempt to connect these two is, to say the least, irrelevant," it said.

Giorgos Koronias, Vodafone CEO in Greece told the parliamentary committee investigating the wiretaps: "There must be an organisation behind this that combines technology and financing. It was not just hackers, this is something bigger. Such know-how does not exist in Greece." The stealth bugging software had been installed at two of Vodafone's main Athens facilities, in Peania and Kifissos.

## Greek government still searching for predator eavesdropping source

Dr Themis Sofos has presented evidence to Athens prosecutor Ioannis Diotis who will soon rule on whether Costas Tsalikidis' death was a suicide or murder. His conclusions will be published later this year.

# mail and Murder

## TAP MYSTERY



Theodore Roussopoulos

alleged suicide of Tsalikidis after the phone-tapping operation was discovered on the Vodafone network.

The operation was apparently detected after a manager had received complaints about "technical problems" from customers. The perpetrators reportedly installed a programme in three Vodafone centres, which intercepted the calls sending them to mobile phones using elusive pay-as-you-go services. The 'ghost' software responsible was then isolated by the multinational Ericsson, which had developed Vodafone's systems, on 7 March 2005.

Many questions remain unanswered, including who actually conducted the phone-tapping and why? Suspicion has

The family of Mr Tsalikidis are convinced his death is suspicious. They have asked for his body, buried in a family plot, to be exhumed enabling independent officials to carry out a second post-mortem. It is understood this would be performed by one of the world's leading forensic pathologists, Dr Michael Baden of the United States. Dr Themis Sofos, the solicitor representing the family said: "They believe they will find new evidence." He also suspects aspects of the original police investigation were questionable. "No one went to the house of Costas, no one took photos and to see the circumstances of his death... no one took fingerprints."

The affair has already made international news, and when Mr Tsalikidis' family filed a lawsuit against "persons unknown for complicity in his murder or suicide," the stakes became even higher. The family believe that even if he was not murdered, it's possible he was subjected to threats or blackmail that may have convinced him the only way out was to take his own life.



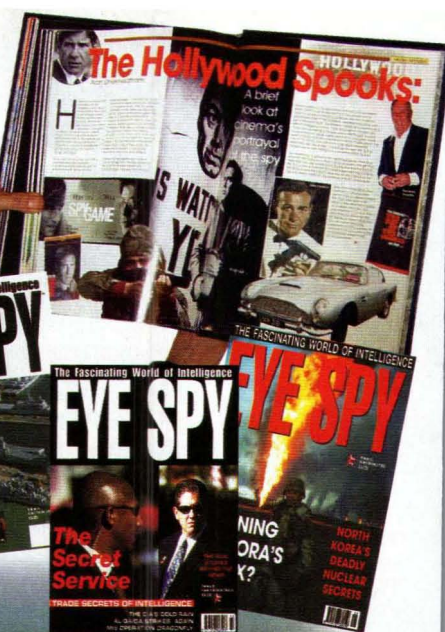
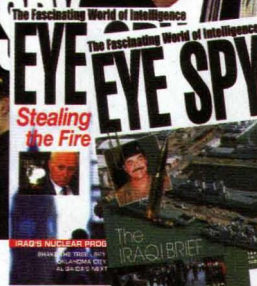
Costas Tsalikidis - found hanged

Sources close to Mr Tsalikidis believe the evidence suggests he was the first person who noticed that "highly sophisticated software" had been covertly uploaded into the Vodafone network in 2004. "The end of January or early February 2005 I think is the time Costas had access [or] had knowledge of the interception system and he searched about its function and origin," said Dr Sofos. "He was not the kind of man to keep secret about something. He would not have co-operated with criminals or criminal acts." During this period, Mr Tsalikidis told his girlfriend, Sarah Galanopoulou, that he must leave



# VOLUME TWO COMPLETE

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



# VOLUME THREE COMPLETE

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

COMPLETE  
YOUR EYE SPY  
COLLECTION



# SUPERB VALUE

ALL VOLUMES COME WITH A FREE EYE SPY  
BINDER AND CD. PRICE INCLUDES P & P  
AND AIR MAIL COSTS TO ALL COUNTRIES!

# VOLUME FOUR COMPLETE

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



OBTAIN THE SECOND, THIRD  
AND FOURTH YEARS ENTIRE  
COLLECTION OF THE  
WORLD'S LEADING AND  
MOST POPULAR  
INTELLIGENCE MAGAZINE



VOLUME TWO (EIGHT ISSUES) NUMBERS 9-16

VOLUME THREE (EIGHT ISSUES) NUMBER 17-24

VOLUME FOUR (EIGHT ISSUES) NUMBER 25-32

Also Available Volume One (Five issues)  
numbers 2, 3, 4, 5 and 8

Ref: ESVOL1 UK £22.50, USA \$45.00 ROW £25.00

Use order form on page 82 or  
order through our secure  
website [www.eyespymag.com](http://www.eyespymag.com)



# THE ATHENS PHONE TAP MYSTERY



his job as it was a "matter of life and death." A text message [sender unknown] on his mobile phone urged him not to leave and offered support.

Investigators are also probing the possibility that it was Tsalikidis himself who allegedly inserted the software enabling the phone-tapping operation. "It is possible," said Themis Sofos. "I cannot exclude anything."

John Brady Kiesling, a former American diplomat posted in Athens at the US Embassy resigned over the 2003 invasion of Iraq. He believes that it is conceivable US intelligence was behind the operation and "it's possible" Tsalikidis was "hired" to install the software. When questioned about his theory, Mr Kiesling said that America simply did not trust the Greeks to provide proper security for the Olym-



Athens prosecutor Ioannis Diotis



managers in Sweden, for activating the law enforcement eavesdropping software package. The parasite conceals that it has activated the eavesdropping package, and conceals its own tracks as well."

**JOHN BRADY KIESLING** writing on his personal web site said: "The bug allows phone calls and SMS messages to be intercepted, and also can track the geographic location of callers (how closely ADAE does not specify). ADAE says this is a generic parasite designed to work with Ericsson software everywhere - proven by the fact that it can exploit software features Vodafone GR does not itself exploit. Designing the bug was a major technical undertaking requiring thousands of man-hours and intimate familiarity with Ericsson telephone software. The parasite bypasses the passwords, allegedly known to only three senior Ericsson



Greek Prime Minister, Costas Karamanlis (right), with Chancellor of Germany, Gerhard Schröder at a NATO Summit meeting. Karamanlis is said to be "incensed" at the spy scandal

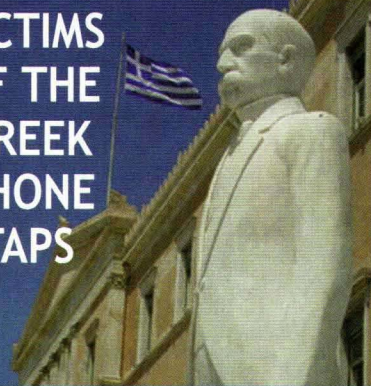
pic Games. "You owe it to yourself if you have the capability, to have an independent ear listening to them and I think that is what this was," said Mr Kiesling.

Officials from the independent Authority for the Protection of Telecommunication Privacy (ADAE) tested the illegal bugging software on 28 February 2006 at the facilities of Ericsson and concluded that only someone who had the codes for Ericsson's legal interception software (on which the illegal bugging software was installed at Vodafone) - which only three Ericsson officials had - could have installed it at Vodafone. The daily newspaper *Ta Nea* published a report on 1 March, citing an anonymous Vodafone source. He reported that the company informed the government in February 2005 that US intelligence agents were involved. The Greek government immediately dismissed the report as "myths".

- In February 2006, Greek Prime Minister Costas Karamanlis announced several measures aimed at mobile phone operators. Companies in breach of the new regulations, aimed at stopping

mobile phone eavesdropping, face fines of up to £1.5 million (\$2.5m) and a temporary suspension of operating licences. "We are preparing more effective safeguards and harsher penalties for those who are involved in such crimes, and for those who make use of the products of these crimes," the prime minister said.

## VICTIMS OF THE GREEK PHONE TAPS



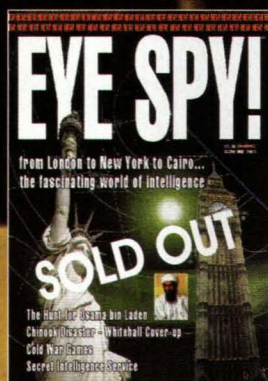
The 46 individuals listed as having fallen victim to the mobile phone tapping include Prime Minister Costas Karamanlis, the foreign minister, defence minister, the public order minister, the justice minister, the deputy foreign minister, former PASOK minister Yiannos Papantoniou, the mayor of Athens, a few journalists, police officials, diplomats, defence ministry cadres and attorneys, as well as mobile phones belonging to ruling officials of the New Democracy party. Other targeted individuals include known anti-state, anti-war or out-of-Parliament left-leaning activists, a Greek-American US Embassy employee, along with 11 individuals with Arab surnames, including a correspondent for Al Jazeera and a former correspondent in Athens for a Syrian newspaper.



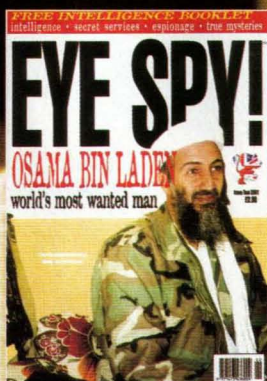
# VOLUME ONE

# VOLUME TWO

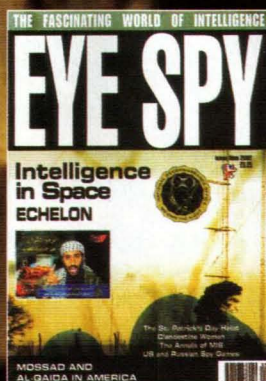
# VOLUME THREE



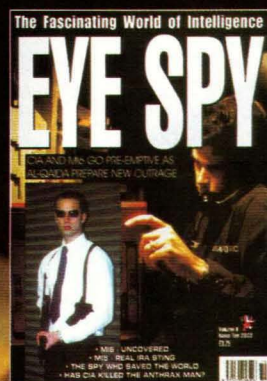
ISSUE 1 REF: ES/01  
USA \$7.00 UK £3.50 EUR €4.50



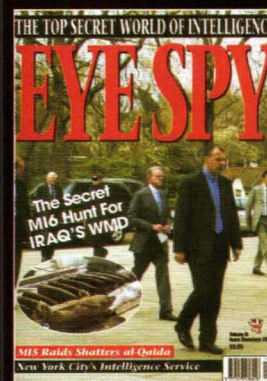
ISSUE 2 REF: ES/02  
USA \$7.00 UK £3.50 EUR €4.50



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



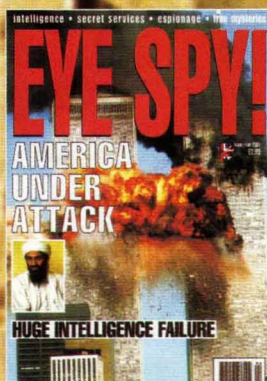
ISSUE 10 REF: ES/10  
USA \$7.00 UK £3.50 EUR €4.50



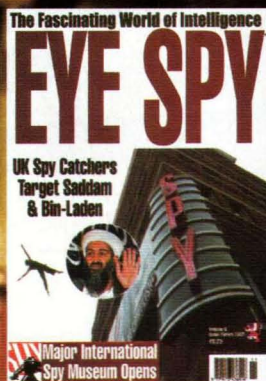
ISSUE 17 REF: ES/17  
USA \$7.00 UK £3.50 EUR €4.50



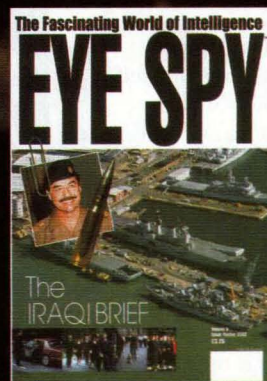
ISSUE 3 REF: ES/03  
USA \$7.00 UK £3.50 EUR €4.50



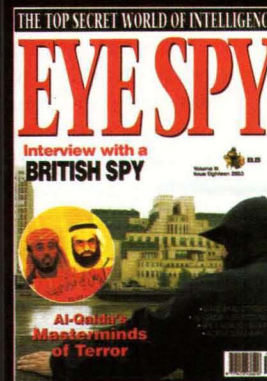
ISSUE 4 REF: ES/04  
USA \$7.00 UK £3.50 EUR €4.50



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



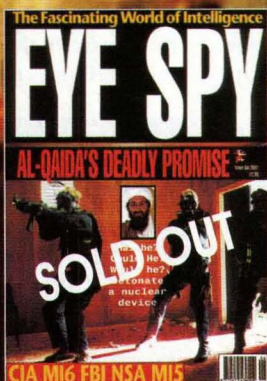
ISSUE 12 REF: ES/12  
USA \$7.00 UK £3.50 EUR €4.50



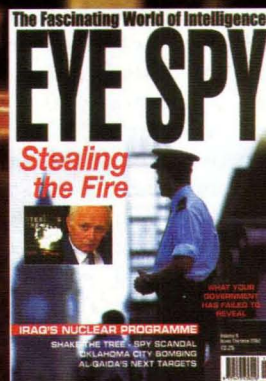
ISSUE 18 REF: ES/18  
USA \$7.00 UK £3.50 EUR €4.50



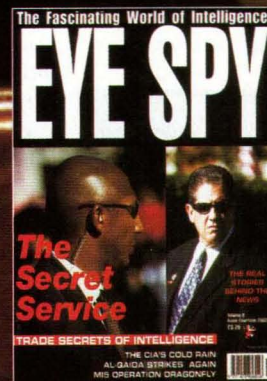
ISSUE 5 REF: ES/05  
USA \$7.00 UK £3.50 EUR €4.50



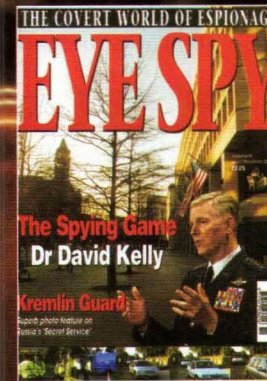
ISSUE 6 REF: ES/06  
USA \$7.00 UK £3.50 EUR €4.50



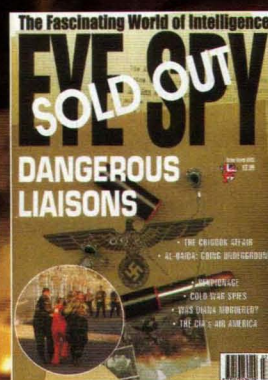
ISSUE 13 REF: ES/13  
USA \$7.00 UK £3.50 EUR €4.50



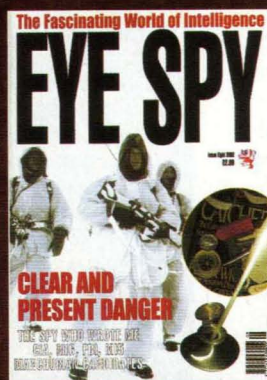
Issue 14 Ref: ES/14  
USA \$7.00 UK £3.50 EUR €4.50



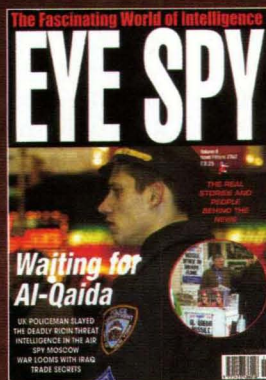
ISSUE 19 REF: ES/19  
USA \$7.00 UK £3.50 EUR €4.50



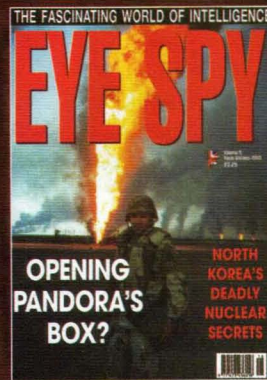
ISSUE 7 REF: ES/07  
USA \$7.00 UK £3.50 EUR €4.50



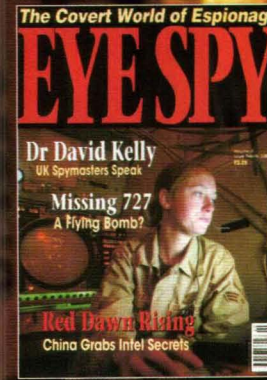
ISSUE 8 REF: ES/08  
USA \$7.00 UK £3.50 EUR €4.50



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

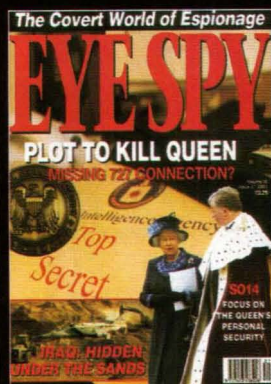
EYE SPY INTELLIGENCE  
MAGAZINE BACK ISSUES



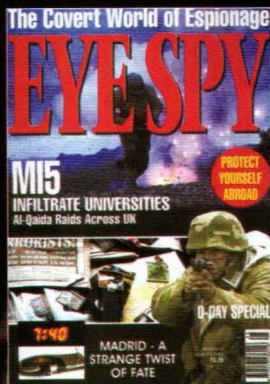
THREE

VOLUME FOUR

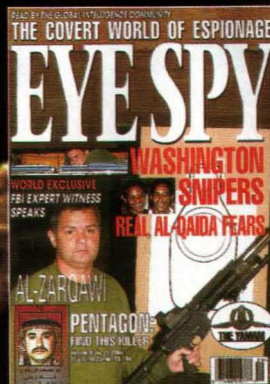
VOLUME FIVE



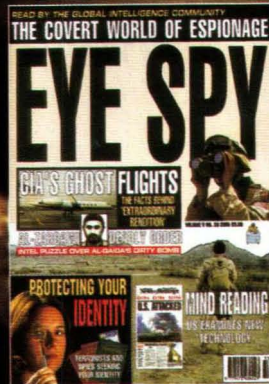
ISSUE 21 REF: ES/21  
USA \$7.00 UK £3.50 EUR €4.50



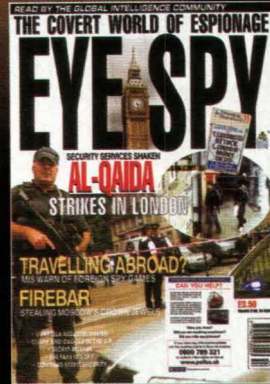
ISSUE 25 REF: ES/25  
USA \$7.00 UK £3.50 EUR €4.50



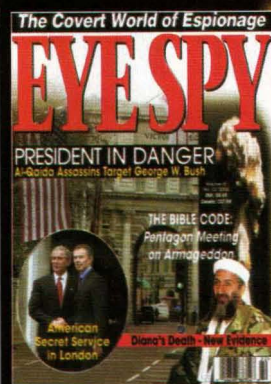
ISSUE 29 REF: ES/29  
USA \$7.00 UK £3.50 EUR €4.50



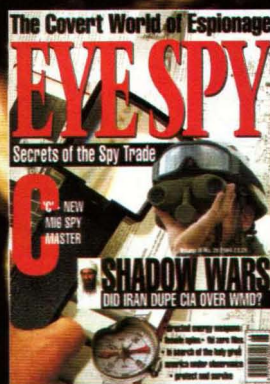
ISSUE 33 REF: ES/33  
USA \$7.00 UK £3.50 EUR €4.50



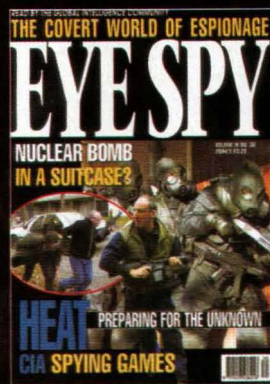
ISSUE 34 REF: ES/34  
USA \$7.00 UK £3.50 EUR €4.50



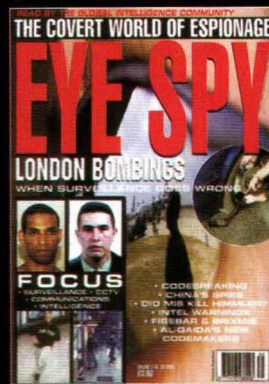
ISSUE 22 REF: ES/22  
USA \$7.00 UK £3.50 EUR €4.50



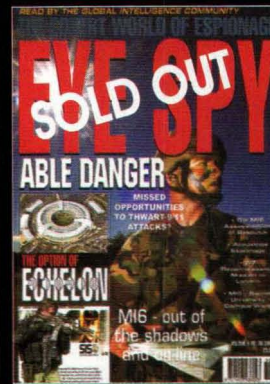
ISSUE 26 REF: ES/26  
USA \$7.00 UK £3.50 EUR €4.50



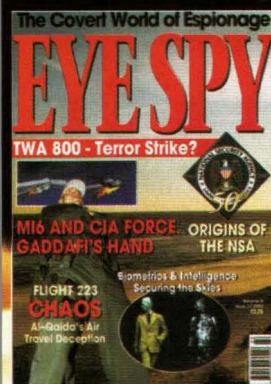
ISSUE 30 REF: ES/30  
USA \$7.00 UK £3.50 EUR €4.50



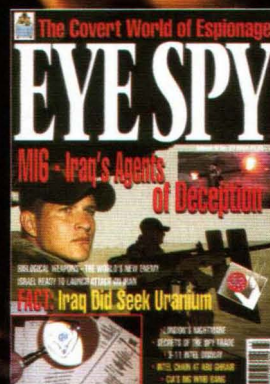
ISSUE 35 REF: ES/35  
USA \$7.00 UK £3.50 EUR €4.50



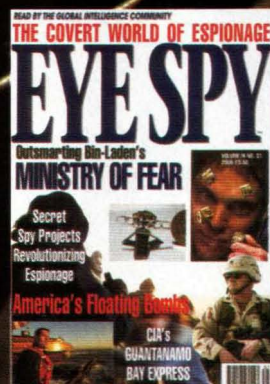
ISSUE 36 REF: ES/36  
USA \$7.00 UK £3.50 EUR €4.50



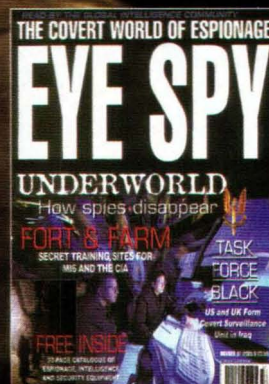
ISSUE 23 REF: ES/23  
USA \$7.00 UK £3.50 EUR €4.50



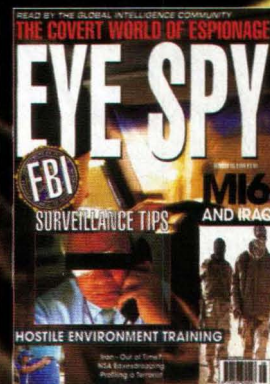
ISSUE 27 REF: ES/27  
USA \$7.00 UK £3.50 EUR €4.50



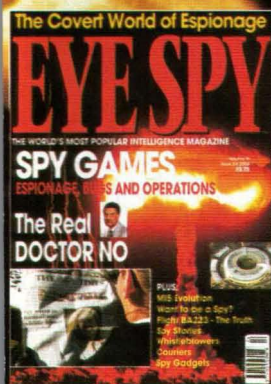
ISSUE 31 REF: ES/31  
USA \$7.00 UK £3.50 EUR €4.50



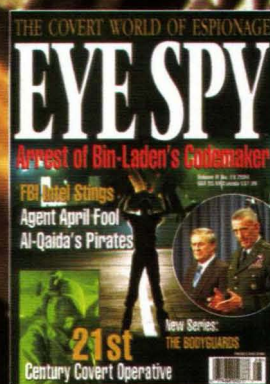
ISSUE 37 REF: ES/37  
USA \$7.00 UK £3.50 EUR €4.50



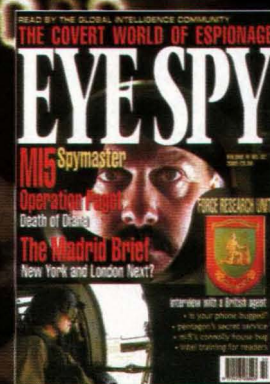
ISSUE 38 REF: ES/38  
USA \$7.00 UK £3.50 EUR €4.50



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



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 39 REF: ES/39  
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.eyespyimag.com](http://www.eyespyimag.com)  
**ORDER BY PHONE:**  
UK, EUROPE AND REST OF WORLD  
TELEPHONE: 01756 770199 (UK)  
NORTH AMERICAN READERS  
TOLL FREE: 877 309 9243

Each highly collectable edition represents a worldwide overview of global events  
- your bridge to the covert world of espionage and intelligence

Require complete volumes? See page 28 and save!



# BODY FOR HIRE

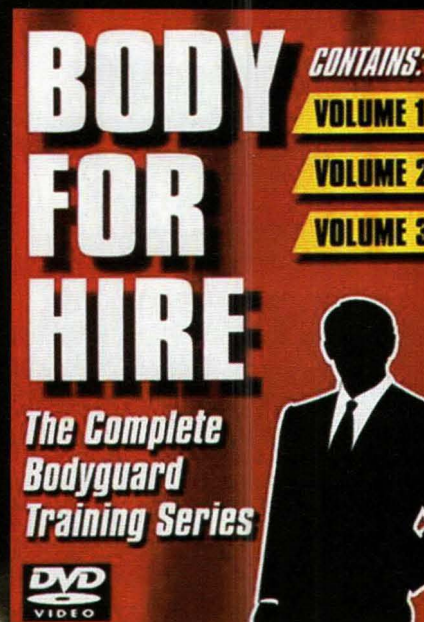
Three Disk DVD Set - Nearly six hours of lessons and training. Starring: Rick Reynolds, Bill Thompson  
Director: James DePalma

## THE COMPLETE BODYGUARD TRAINING SERIES

**VOLUME #1** Filmed during actual classes. Lessons taught in this video include: professional clothing, weapons selection, how to select a client, when to decline a contract, how to tell if the client is hiding critical information from you, what acronym tells you what to do in a deadly encounter, four topics for a successful assignment, press and media relations, professional terminology, protective formations, team placement, motorcade operations, advance security surveys, coordination with other security details, and explosives search methods. 1 hour 50 minutes

**VOLUME #2** Lessons include: vehicle pre-flight inspections, selecting the right vehicle, limousines, cars and vans, emergency evacuations, how to brief your client, precision driving techniques including J-turns, bootlegs and speeding, ramming roadblocks and barricades, preventing vehicle ambushes, firearms CQB, headshots, weapon retention, shooting through glass, firearms carrying and drawing techniques, and walking (guarding) the principal. 1 hour 50 minutes

**VOLUME #3** This video contains more advanced lessons in communications selection and safeguards, hotel and restaurant security, dining etiquette, surveillance and counter-surveillance, threat assessments, vehicle bomb searches, advance survey checklists, and safeguarding proprietary information. 1 hour 50 minutes



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

Ref: BFH/3 US \$125.00 - use  
order form on page 82

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

## EYE SPY'S COVERT CAMERA Inside industrial smoke detector -

**SPECIAL READER OFFER**

**SAVE**

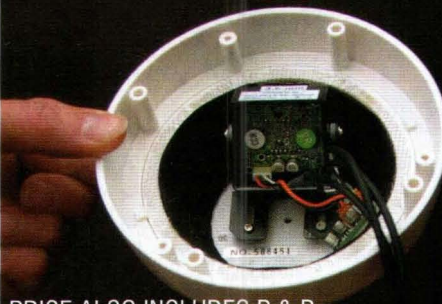


"Easy to install, very reliable and works brilliantly"  
- Peter Jenkins, author of Advanced Surveillance



Covert Monochrome Camera housed in an industrial smoke detector. Features: CCD - 1/3" Res - 380 Lines Lux - 0.1 Lens - 3.6mm Add - Supplied with BNC/Power Cable Power - 12V DC Dims (mm) - 130 Dia x 57 Weight - 0.3Kg (Audio - Optional - call Eye Spy)

Camera only - was £149.95 now **£125.95**  
(order code ES/CCSM)  
With 18m cable & PSU - was £169.95  
now **£140.95** (order code ES/CCSMCAB)



PRICE ALSO INCLUDES P & P  
UK READERS ONLY



# EYE SPY SHOP



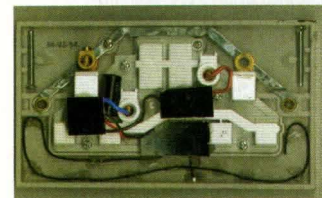
**MAINS-DOUBLE  
SOCKET  
TRANSMITTER**

**PROFESSIONAL**

Professional surveillance and espionage equipment available from Eye Spy.

Check out our new range of products on: [www.eyespy.com](http://www.eyespy.com)

## 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**

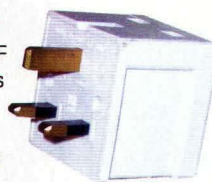
Order Code: LS-CCT UK £195.00  
USA \$350.00 ROW £199.00

### 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. 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

### 12-CHANNEL METAL CASED UHF RECEIVER UNIT



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

Eye Spy's superb 12-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](http://www.eyespy.com)**



*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.*



### 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



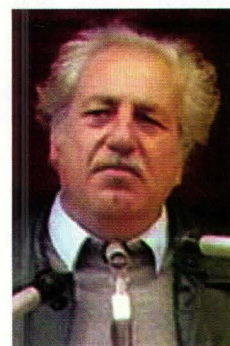
# LOCKERBIE BOMBING

## WHO WAS BODY 59 - DCF12?

According to campaigners urging the release of convicted Pan Am bomber Al Megrahi, "earth shattering" information has been found that will create grounds for a major review of the case - including the circumstances which brought down Flight 103 over the Scottish town of Lockerbie in 1988. Over 250 people died in the terrorist attack, but not everyone feels justice has been done...

**F**ew people involved with the recovery of bodies after terrorists brought down Pan Am Flight 103 on 21 December 1988, will ever forget the scene. The huge airliner tumbled out of the sky scattering lifeless corpses for miles around. All 259 persons and crew on board the aeroplane, and a further 11 people in the Scottish town of Lockerbie died. Amazingly, nearly all were later identified and their remains returned to loved ones.

Rumours abounded over who actually authorised and carried out the attack. Initially Iran was suspected because in July 1988, the US Navy battle cruiser Vincennes accidentally shot down an Iranian Airliner over the Persian Gulf, killing all 290 people on board. Elements in the Tehran government reportedly commissioned a Syrian-based group, the Popular Front For The Liberation Of Palestine General Command (PFLP-GC) to carry out a revenge attack.



Ahmed Jibril -  
headed PFLP-GC

### AUTUMN LEAVES

PFLP-GC bomb-maker, Marwan Khrebat, was sent to Germany and assembled five bombs designed to detonate at high altitude. Unbeknown to Khrebat, German police were watching his every



move. On 26 October he and 14 other PFLP-GC suspects were rounded up in an operation code-named Autumn Leaves. A device, built into a Toshiba radio-cassette player, was seized. However, the weight of evidence soon pointed to Libya, though the significance of the cassette player would soon return.

Libyans Abdul Baset Ali al-Megrahi and Al-Amin Khalifa Fhimah were eventually charged. Both men had connections to Libya's intelligence agency - JSO. Controversy still reigns as to how they planted the device, however, many intelligence watchers believe the men were 'implanted' in the offices of Libyan Arab Airlines at Malta's Luqa Airport. Prosecutors said they secreted the bomb inside a Toshiba radio cassette which was in turn put in a Samsonite suitcase and loaded on an Air Malta airliner at Frankfurt Airport. That bag was then put on board Pan Am Flight 103.

#### SEARCHING FOR CLUES

Following the incident, forensic specialists searched for the tiniest clue that could explain what happened. The



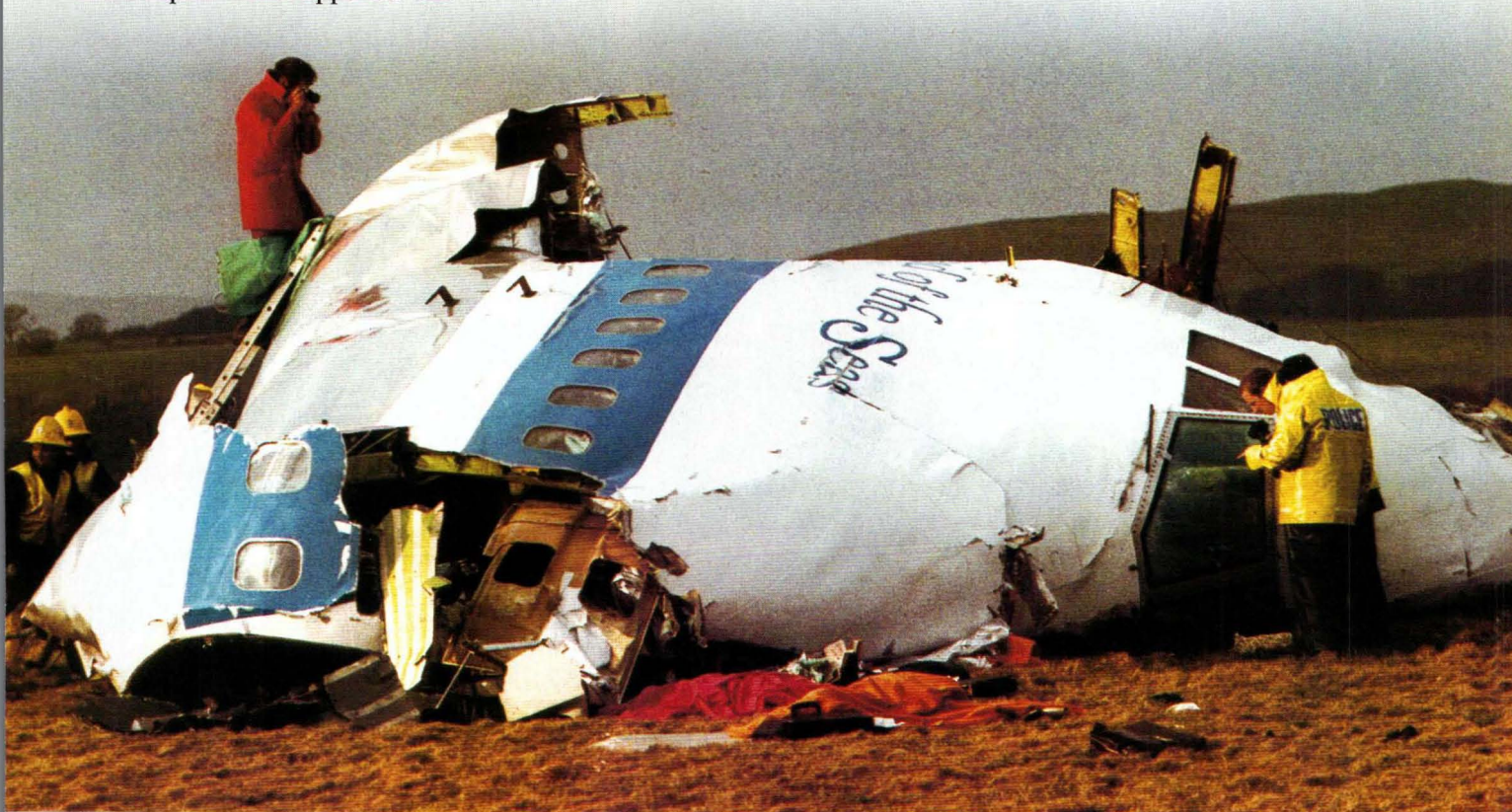
Above: Clothes found in the debris were traced to a Maltese merchant, Tony Gauci, who became a key prosecution witness, testifying that he sold the clothes to a man of Libyan appearance, whom he later identified as Al Megrahi. This photo was shown to Gauci.

© CROWN COPYRIGHT

Colonel Gaddafi denied that his country was involved in the destruction of Pan Am Flight 103. However, in 2003, following the lifting of UN sanctions, Libya agreed to pay the victims families millions of dollars in compensation

speed of the destruction of the airliner indicated terrorism, thus specialist personnel joined the search teams. Clothing was recovered that contained the residue from the explosive Semtex. A label marked 'Malta Trading Company' led detectives to a small shop on the island of Malta, where the shop owner said a man resembling Al-Megrahi had bought similar clothing... but he couldn't be 100 per cent certain.

Another clue to the bombing was found in Switzerland. Edwin Bollier, whose Zurich-based company - 'Mebo' made timers. MI6 and the CIA were convinced that debris, including a tiny piece of circuit board, presumably from the timer, was manufactured by Mebo. Though Bollier agreed, it was crucial to make a connection. It was learned that this particular timer was sold to Libya and East Germany. Al-Megrahi and





# THE VINCENNES

## Air Incident 1988

**T**he USS Vincennes was involved in the tragic shooting down of Iran Air Flight 655 (IR655) amidst rising tension between the USA and Iran. All 290 passengers and crew on board the aircraft were killed.



IR655 was a commercial flight operated by Iran Air that flew from Tehran to Bandar Abbas to Dubai. On 3 July the plane, an Airbus A300B2, registered as EP-IBU and flown by captain Mohsen Rezaian, left Bandar Abbas at 10.17am Iran time, some 27 minutes after its scheduled departure time of 9.50 am. It would have been a 28-minute flight. At that same time, the USS Vincennes, under the command of Captain William C. Rogers III and fitted with the AEGIS combat system, was nearby in the Strait of Hormuz.

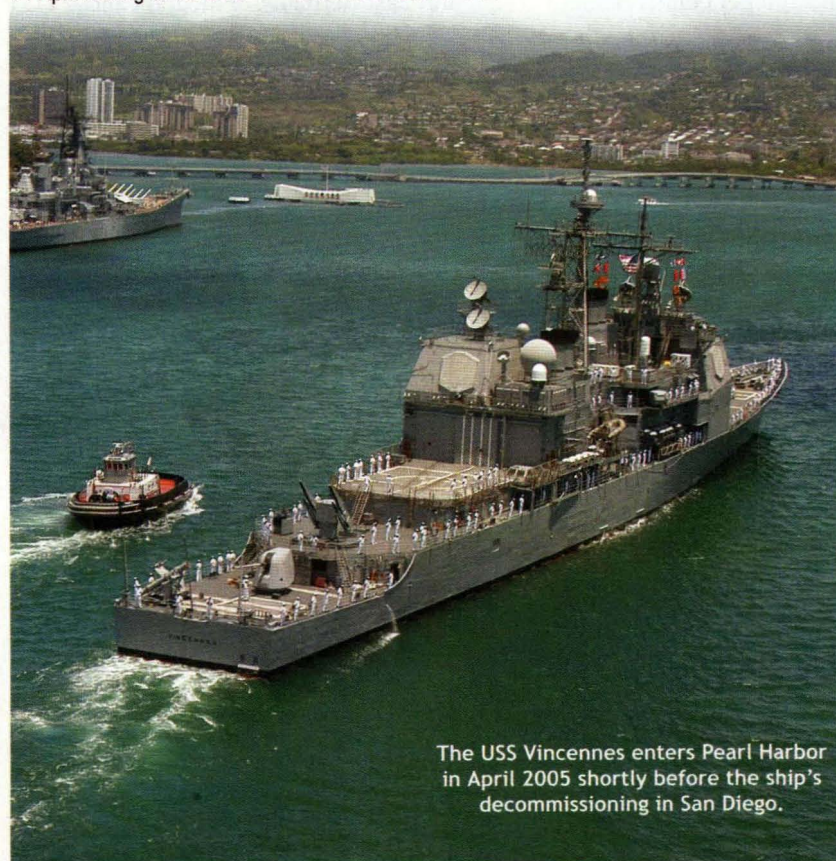
The Vincennes had been rushed to the area after the 14 April mining of the USS

Samuel B. Roberts by Iranian forces. Roberts had been operating in the Persian Gulf as part of Operation Earnest Will, the effort to protect Kuwaiti oil tankers during the Iran-Iraq War. In response to the Tehran's action, two Iranian warships were sunk.

On the morning of 3 July, the Vincennes clashed with Iranian gunboats. The Vincennes' control room then reported an unidentified aerial target approaching and checked with air flight departure logs to try and identify the aircraft. Officers identified the flight profile being flown by the A300B2 as being similar to that of an Iranian Air Force F-14A

Tomcat. The Vincennes tried to make contact with the aircraft, though at that time it had no equipment suitable for monitoring civil aviation frequencies, other than the International Air Distress frequency. After failing to make contact with the aircraft the Vincennes captain ordered the launch of two SM-2ER anti-aircraft missiles. It was apparent within minutes a dreadful mistake had occurred.

Three years later the US admitted the Vincennes was inside Iranian territorial waters at the time of the shoot-down.



The USS Vincennes enters Pearl Harbor in April 2005 shortly before the ship's decommissioning in San Diego.



Abdul Baset Ali al-Megrahi

## LOCKERBIE

## BODY

## DCF12

Khalifa Fhimah said they believed Palestinian terrorists were involved. At the time, the East German security service Stasi backed many Palestinian groups, thus it was possible, though unlikely, the communist state supplied the timer used in the Lockerbie bomb. In the end, Libyan leader Colonel Gaddafi handed over the two suspects. Al-Megrahi was sentenced to life imprisonment, while Khalifa Fhimah was cleared of all charges.

Since then, rumours have abounded and some people believe Al-Megrahi, who remains in jail, is innocent.

One man, closely associated with the case, is former police surgeon Dr David Fieldhouse. He travelled to Scotland from his home in Yorkshire just hours after the crash site to help label bodies. Apparently he counted and carefully issued numbers to 59 corpses, but when the final tally came in, official documents note that only 58 were tagged. Speaking recently to journalists, Dr Fieldhouse believes the missing body - tagged DCF12 is relevant to the incident and was removed by persons unknown. He also believes that Al-Megrahi is part of a wider, murkier affair and that agencies, including the CIA, had a "lot to cover up".

At the time, the incident appeared an open and shut case, insofar as terrorism was concerned. Then followed a number of investigations, and an apparent drugs connection emerged. This was even raised in Parliament in the mid-1990s, though it was never satisfactorily explained. Even today, Dr Fieldhouse thinks this is relevant. "There might also have been some connection with the drug route. Something was going on, but everyone clammed up," he said.

That "drug route" mentioned by Dr Fieldhouse, relates to information uncovered by Juval Aviv, a private investigator hired by the now defunct Pan Am to help identify those responsible for blowing up the airliner. His investigation left open the



# Juval Aviv's Pan Am Report

**T**he 27-page report prepared by Juval Aviv for Pan Am makes interesting reading. In 1987, Aviv writes, US agents discovered and began monitoring a heroin-smuggling route from the Middle East to the United States, via Frankfurt, run by a Syrian drug and arms-dealer named Monzer al-Kassar. Al-Kassar had ties to Hizbollah terrorists who held Western hostages in Beirut. US agents allegedly agreed to let al-Kassar's heroin operation run -

through Frankfurt and London's Heathrow airports - in return for al-Kassar's promise to help free hostages.

Aviv claims Khalid Jaafar, a young Lebanese-American killed on Pan Am 103, was a regular courier for al-Kassar's operation. Ahmed Jibril of the Syria-based PFLP-GC knew of al-Kassar's successful drug route when he began plotting with his sponsors in Iran to avenge the Vincennes shoot-down, the report

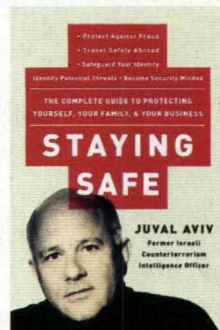
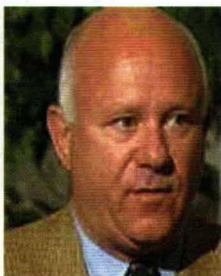
asserts. It says Jibril, after considering other US carriers, ultimately decided to blow up Pan Am 103 by, in effect, horn-in on al-Kassar's government-controlled smuggling operation. The PFLP-GC allegedly used baggage handlers at the Frankfurt airport to replace Jaafar's heroin bag with a bomb-laden suitcase, according to Aviv's scenario.

In response to Aviv's report, and investigative news stories based on them, government officials launched an attack on Aviv that went well beyond simple denials. In letters to newspaper editors



and on network TV, diplomatic and intelligence officials called Aviv a "fabricator" who had lied about his entire background.

Aviv, a 30-year security veteran is author of the book - 'Staying Safe'.



possibility that members of the PFLP-GC took advantage of a controlled drug-smuggling route involving US agents in Frankfurt, to put the bomb on Flight 103. It was a claim vehemently denied by the United States Government - and still is. In response to Aviv's report, Pan Am filed subpoenas with several US intelligence and law enforcement agencies, seeking documents to confirm or refute the private investigator's findings. The government refused to release the documents on grounds of national security. As for Aviv, he said: "I was a consultant to the FBI for over ten years on anti-terrorism matters. Once I pointed the finger at the government, I became persona non grata, my arrangements with the FBI were cancelled. I just became a government enemy."

In 1994, former FBI Director of Investigations 'Buck' Revell was asked if US agents ran operations in cooperation with Middle East drug dealers around the time of the Pan Am attack. "There was intelligence being gathered," Revell said. "DEA

[Drug Enforcement Administration] assets were tasked by orders from the National Security Council to try to develop intelligence information on American hostages in Lebanon. They were not used in conjunction with Pan Am 103. That entire operation had been closed down."

Dr Fieldhouse believes his 'missing' body - DCF12 - is a major clue - that the body was removed to conceal its identity. He even refers to a mysterious coffin-shaped box being quietly "shipped out" of the English border town of Carlisle just after the search had concluded. In the next few weeks he is returning to Scotland to discuss "new evidence" that might cast doubt on the original verdict against Al-Megrahi, which he described as "staggering."

Retired MP Tam Dalyell (right), who first raised Dr Fielding's concerns in Parliament in 1995, believes there has been a miscarriage of justice (see sidebar). "The Crown Office has simply put up the shutters against anything new because it

has already had its triumph in court. But this man in prison [Al-Megrahi] has nothing to do with the Lockerbie crime... and they know it."

Conspiracy theories persist, but did Dr Fieldhouse make a genuine mistake in counting the number of bodies he tagged? "At its very simplest I may have made a mistake... but I don't believe I did," he said.

• In September 2003, the UN Security Council lifted sanctions against Libya, which allowed the release of up to \$2.7 billion to the families of the 270 people killed. Libya paid each family \$8 million in compensation and was scheduled to pay a further \$2 million to each of the victims' families.

## HOUSE OF COMMONS HANSARD 16 OCTOBER 1995

Mr Dalyell: To ask the Secretary of State for Scotland if he will now specify the quantity and nature of the drugs found in the debris near Lockerbie after the destruction of Pan Am flight 103. [37394]

Lord James Douglas-Hamilton: The hon. Member is referred to the answer given on 6 March 1995, Official Report, column 87.

Mr Dalyell: To ask the Secretary of State for Scotland what guidance the Crown Office gave to the deputy chief constable of the Dumfries and Galloway police in responding to the letter from the former Bradford police surgeon, Dr David Fieldhouse, regarding the failure to make further inquiry of him about body DCF12, labelled by Dr Fieldhouse at a hillside north-east of Shawhill farm, Lockerbie, on 22 December 1988. [37460]

Lord James Douglas-Hamilton: Communications between the prosecuting and Investigating authorities are confidential.



© LAW ENFORCEMENT PICTURE LIBRARY/STEVE MCMAHON



# 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@eyespymag.com](mailto:eyespy@eyespymag.com) **ONLINE** [www.eyespymag.com](http://www.eyespymag.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:

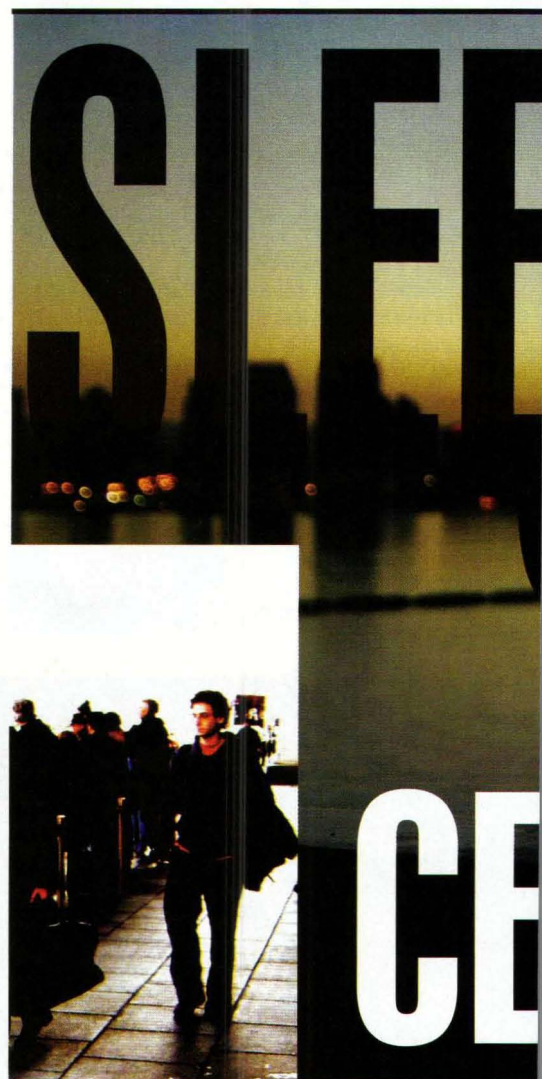
**Eye Spy International**

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



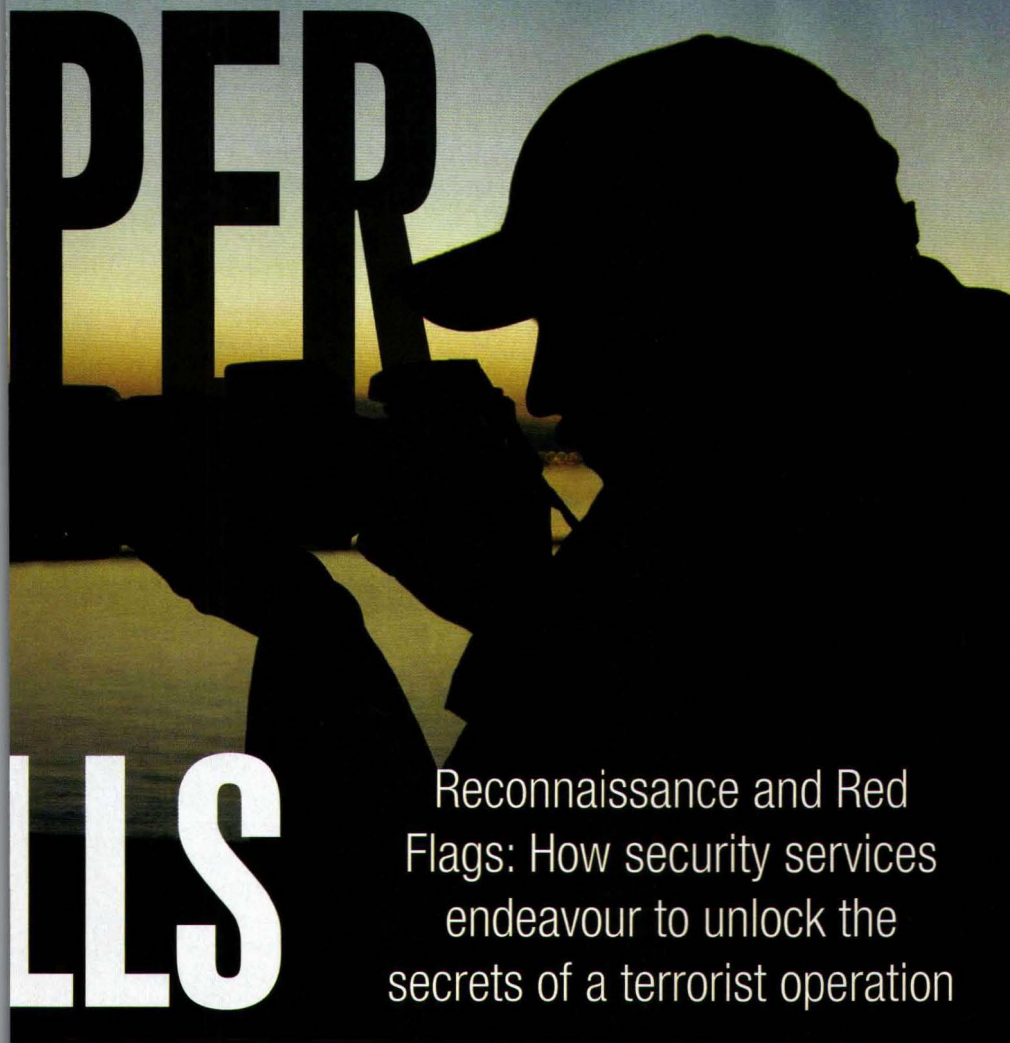
**J**ust weeks prior to the bombings in London in July 2005, three of the four terrorists travelled to the capital in what was described as a "dry run" - a reconnaissance mission.

Attention to detail was everything - confirming train times, wearing the correct clothing, carrying rucksacks, practising looking relaxed etc. And though London is a crowded city at the best of times, the bombers picked a time when the Underground was at its busiest. This was no coincidence but a carefully managed decision.

Few details (if any), will ever be released by MI5 and Scotland Yard on the intelligence gleaned by investigative officers. The data will be disseminated and included to augment existing files that enable officers and analysts to identify and thwart future operations. Sadly, they will also be used to investigate crimes that are not stopped.

In the last 12 months, the public in the UK have often read about "terror arrests" in their newspapers, or heard brief snippets on the radio and televi-





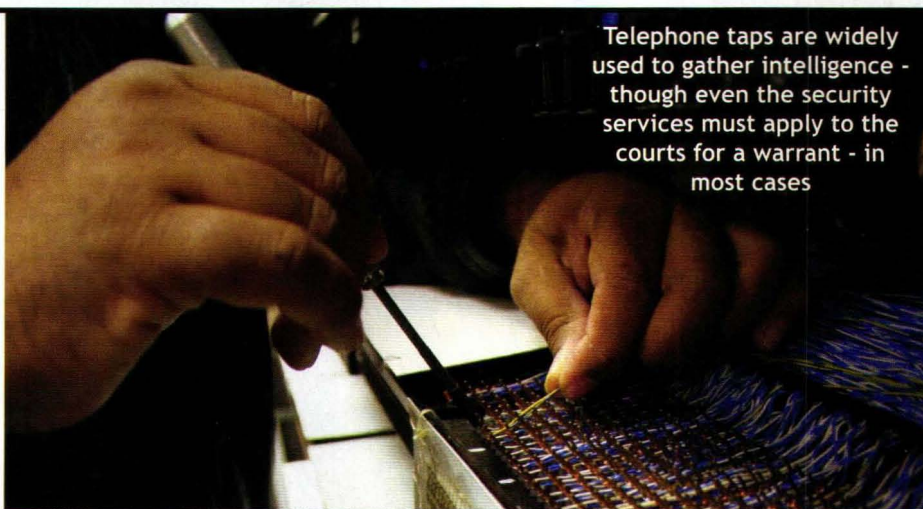
## Reconnaissance and Red Flags: How security services endeavour to unlock the secrets of a terrorist operation

are simply out of touch with the often complex work needed to gather further intelligence. A case in question is the terror suspect with nearly 30 identities. It was impossible for officers to check each and every one in the time frame set. In the end he was released and left the UK. Months later it was learned he was already wanted by a European country for his links to terrorism. Every aspect of gathering intelligence and clues on a potential suspect must be thorough. However, this is also problematic as vast resources are needed for each operation.

Surveillance can take many forms, but it always entails gathering as much intelligence as possible: who the target meets, shops and businesses visited, the vehicle or transport used and even what type of clothing he wears. Creating a picture is of primary importance, indeed, much can be learned from monitoring his lifestyle. If the officers deem the target is of 'national importance' they can apply for a warrant to intercept phone calls and mail or bug his apartment. If overseas connections are apparent, other agencies such as GCHQ, Interpol and foreign intelligence services may be asked to help.

sion about suspects being detained under the Prevention of Terrorism Act. Sometimes, the suspects (after investigation) are released without charge, on other occasions charges are brought by the Crown Prosecution Service. In both instances, MI5 (the Security Service) has acted because it has either received or gathered intelligence. When police raids occur, they are usually timed to prevent possible incidents happening.

When a suspect is placed under surveillance, intelligence is gathered on a wide range of subjects. Background



Telephone taps are widely used to gather intelligence - though even the security services must apply to the courts for a warrant - in most cases



checks are immediately initiated, but this is just a tiny fraction of the work done by officers to understand if the target is involved with terrorism, crime or underworld activity. There was much debate in Britain in 2005 over the length of time a suspect could be held without charge. The security services requested 90 days, but the court ruled about 28 days was "sufficient." Sadly those in high places

Officers will spend hours, weeks, days and even months surveilling a target. Once he becomes more 'active', additional offices may be deployed to gather every scrap of information that may expose or negate his real intent. MI5 and the FBI, for example, have an extraordinary large manual on counter-measures tactics used by terrorists, drugs aficionados and criminals. If the subject uses any of these, police suspicions may be confirmed. The security services also rely heavily on information



passed to them from the other sources, including the public, as this scenario, based on actual case studies shows.

### THE SLEEPER CELL

Two persons were contacted by an al-Qaida link man to reconnoitre a major building in New York City. Their objective was to gather as much intelligence as possible about the building's security weak points, transport in and out of the cargo docks, the types of uniform worn by building security staff, CCTV positions and note the regular police road checks. Used by government personnel, the building was regarded as a high profile target. Nevertheless, it was a fairly 'secure' place to work.

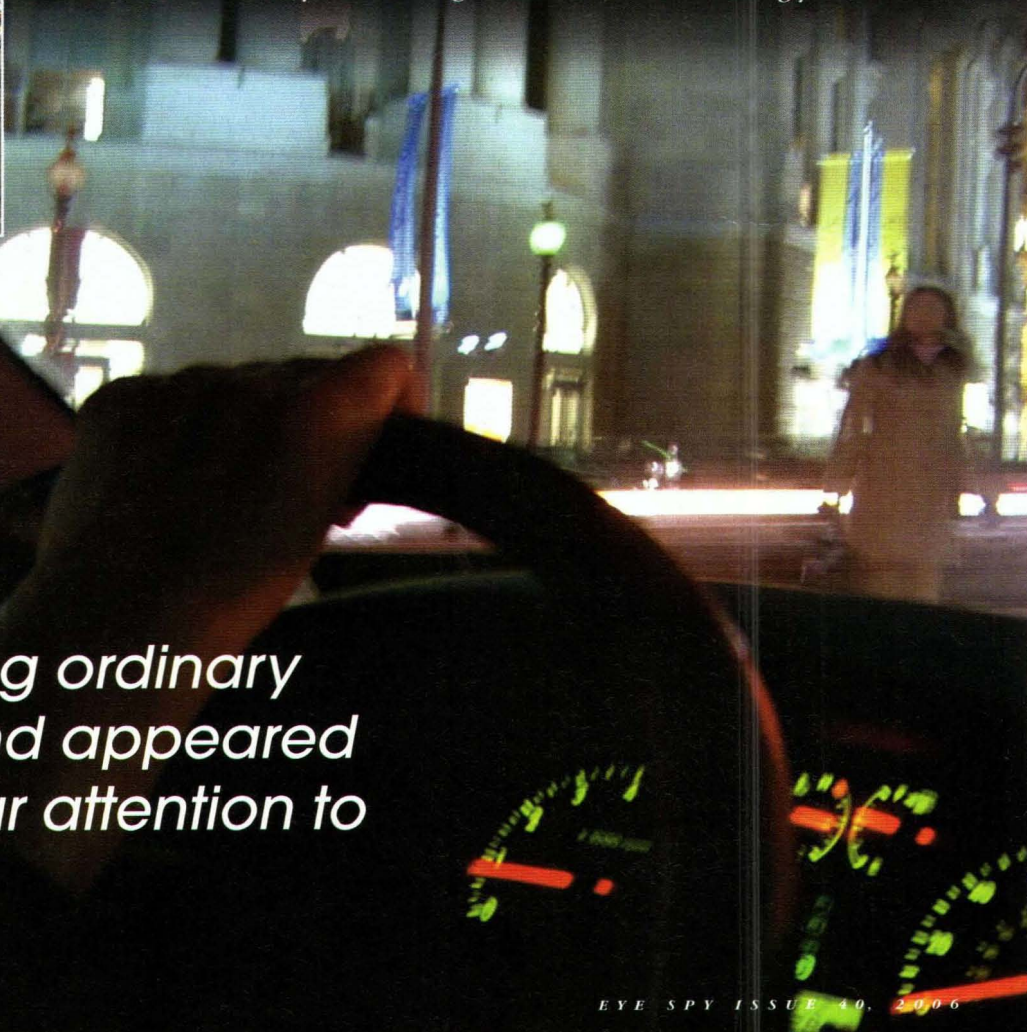
The pair also had to check road approaches, traffic light signals, parking restrictions and what types of vehicles enter and exit the underground car park and main entrance point. Ultimately, they had to determine the best location to park a vehicle that would be used to attack the building. They also had to find an escape route - literally the best way to flee from the scene without being noticed.



The security services became aware of one man when a local taxi firm explained an unusual request (and actions) from a customer who said he was a tourist. After picking the man up in Midtown Manhattan, the customer asked to be driven to a business area of the city. On their arrival, the cab driver was asked to drive around the area twice. The passenger, who wore sunglasses, a baseball cap and appeared vigilant, was armed with a video camera and map. He began filming ordinary street scenes and appeared to pay particular attention to one building. Seconds later he asked to be dropped off a few blocks away. The driver was perplexed, but took his fare and continued on his way. That evening

he read a report in his newspaper about a terrorist alert, and an FBI statement that warned about potential terrorist sleeper cells operating in the city. The next day he reported the incident to his superiors. They duly contacted the police and a report was made.

A few days later the police received a phone call from a cafe owner in the same area. Two men had spent a couple of hours sipping coffee and looking out of the window. Occasionally one man would start filming while the other seemed to be taking notes. Eventually they departed. The cafe owner explained to police the men appeared intense and were seemingly more



*He began filming ordinary street scenes and appeared to pay particular attention to one building...*





ISS TRAINING LIMITED Est. 1990

# THE WORLD'S LEADING SURVEILLANCE TRAINING COURSES

interested in events happening outside. A description of the men was given to the police. One man resembled the customer picked up by the taxi driver.

Though the incidents could be mundane, the information came to the attention of counter-terrorism detectives. They had been informed by the FBI that a report had been received from the CIA. MI6 had provided intelligence on an intercepted signal that may have activated a sleeper cell in the city.

Earlier that week, detectives had visited a vehicle storage lot some twenty miles outside the city after the manager complained of a strange odour. Officers found the vehicle's boot had been used to transport fertiliser or a similar substance. Further enquiries revealed the car had been hired several weeks earlier by two men who said they were tourists. It had been reported stolen after the men had failed to return it to the hire company. There did not seem a connection, though one officer said the fact that the two men - supposedly tourists - were seemingly now on foot.

Forensic specialists examined the fertiliser and sales checks were

*Continued on page 73*



**ISS trainers  
are former regular  
military and police  
surveillance  
operators**

- UK Enforcement Agencies
- Foreign Military Units
- Specialist Agencies
- Private Investigators
- Security Consultants
- Investigation Agencies
- Countermeasures Agencies
- Local Authorities
- Close Protection Officers
- Intelligence Guidance



*For an information brochure and  
course details:*

**ISS Training Limited, Riverside Cottages,  
Nidd Walk, Pateley Bridge, Harrogate,  
North Yorkshire, HG3 5NA  
United Kingdom**

**Tel: +44 (0)1423 - 712265  
email: intel@intelsecurity.co.uk**



# TRIPWIRE

## Pandora's Nuclear

**T**ehran has warned it would use its long-range Shahab-3 missiles to strike Israel or Western forces stationed in the Gulf region if its nuclear sites are attacked or sabotaged. While Iranian President Mahmoud Ahmadinejad, continues to deflect worldwide criticism of Iran's controversial nuclear programme, his military commanders raised the stakes. In a televised address to the Iranian public, General Yahya Rahim Safavi (right) said: "The world

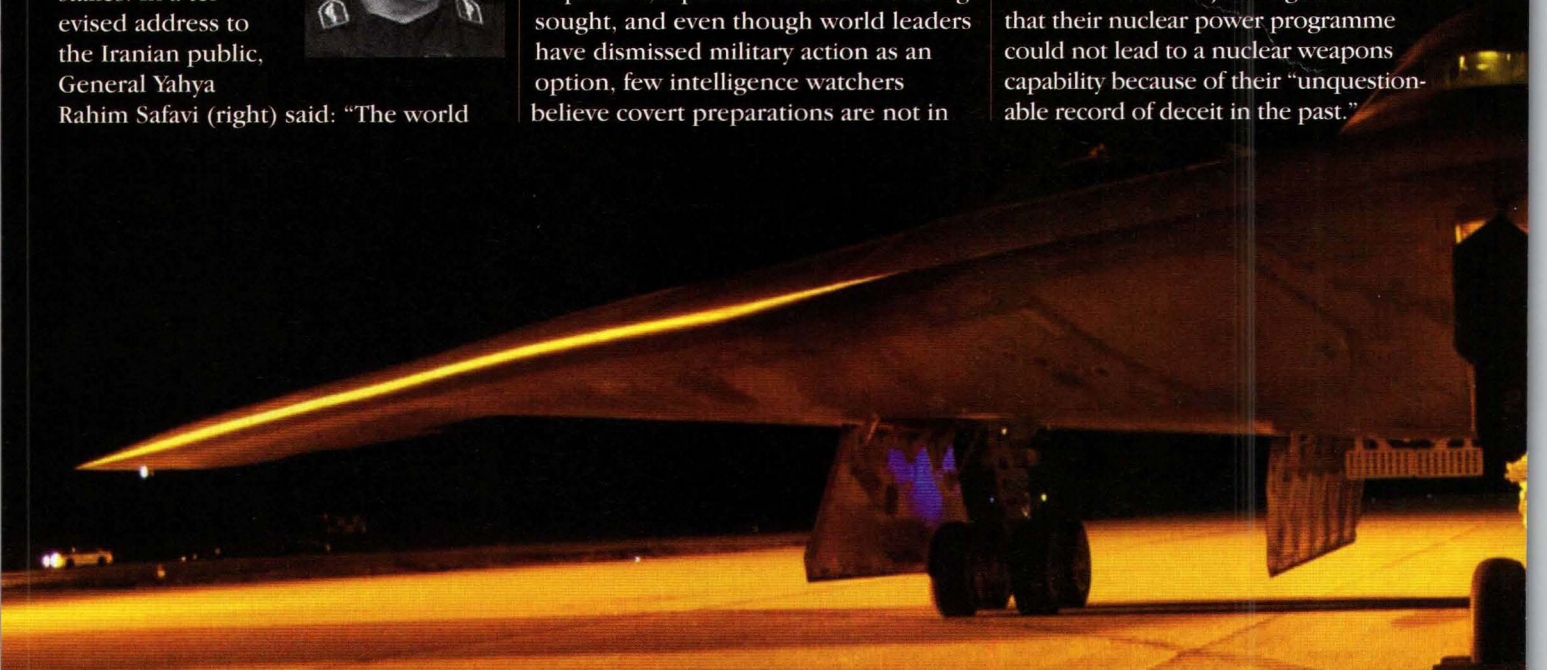


knows Iran has a ballistic missile power with a range of 2000km. We have no intention to invade any country [but] we will take effective defence measures if attacked." A Tehran military official also revealed that Iran would use suicide bombers on the streets of Britain if its nuclear sites were attacked.

Military and intelligence analysts are undecided if Tehran is but two or ten years away from developing a nuclear bomb, but have warned that a 'tipping point' will soon be reached when any chance of using military action to remove Iran's nuclear sites will be lost. At present, a political outcome is being sought, and even though world leaders have dismissed military action as an option, few intelligence watchers believe covert preparations are not in

hand. Indeed, Israel has already conducted a covert exercise that involved air force fighters and Special Forces. "If required, the plans are already in place to 'lessen' the danger," intelligence sources claim. "Iran does not believe an air strike is likely, but it is concerned about sabotage," another analyst told Eye Spy.

Jack Straw, the British Foreign Secretary, conceded that Britain and the US were divided over using military force. "There isn't a military option. And no one is talking about it," said Mr Straw in response to a question about the possibility of using force. However, Mr Straw said there had to be "objective guarantees" that their nuclear power programme could not lead to a nuclear weapons capability because of their "unquestionable record of deceit in the past."

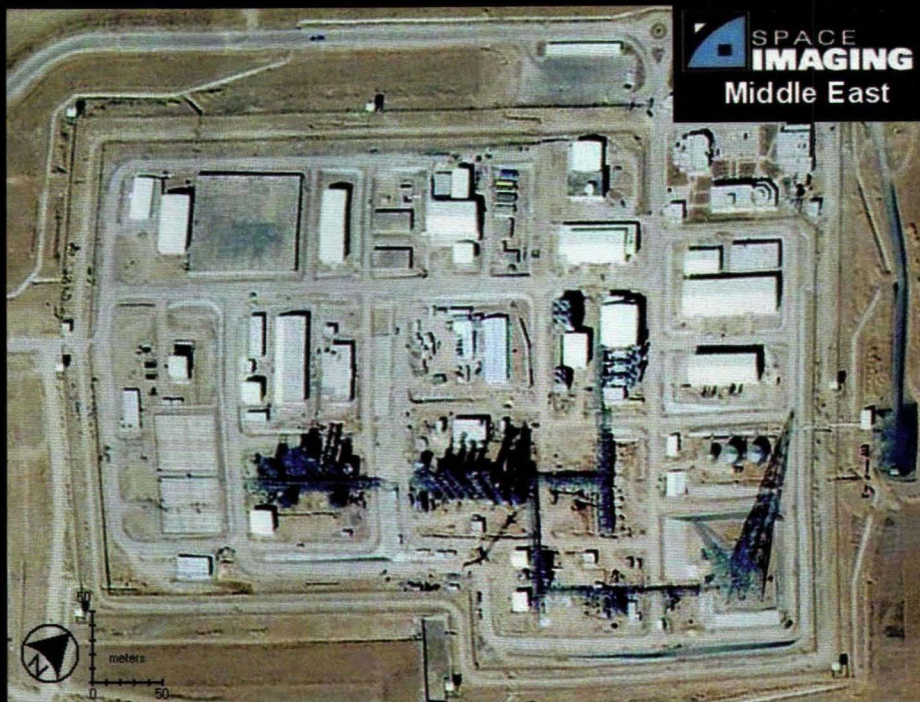


# Iran warns against m

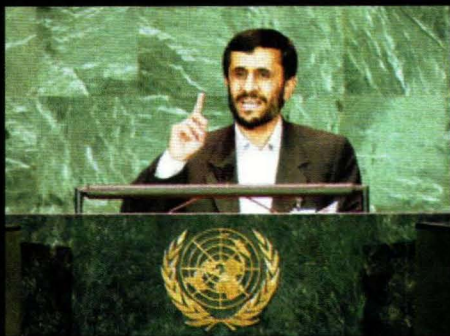


# RE Box

SPACE  
IMAGING  
Middle East



Arak nuclear site: New imagery reveals marked progress on the construction of the production line and the addition of a Hydrogen Sulphide discharge tower. Space Imaging 29 February 2004



President Mahmoud Ahmadinejad

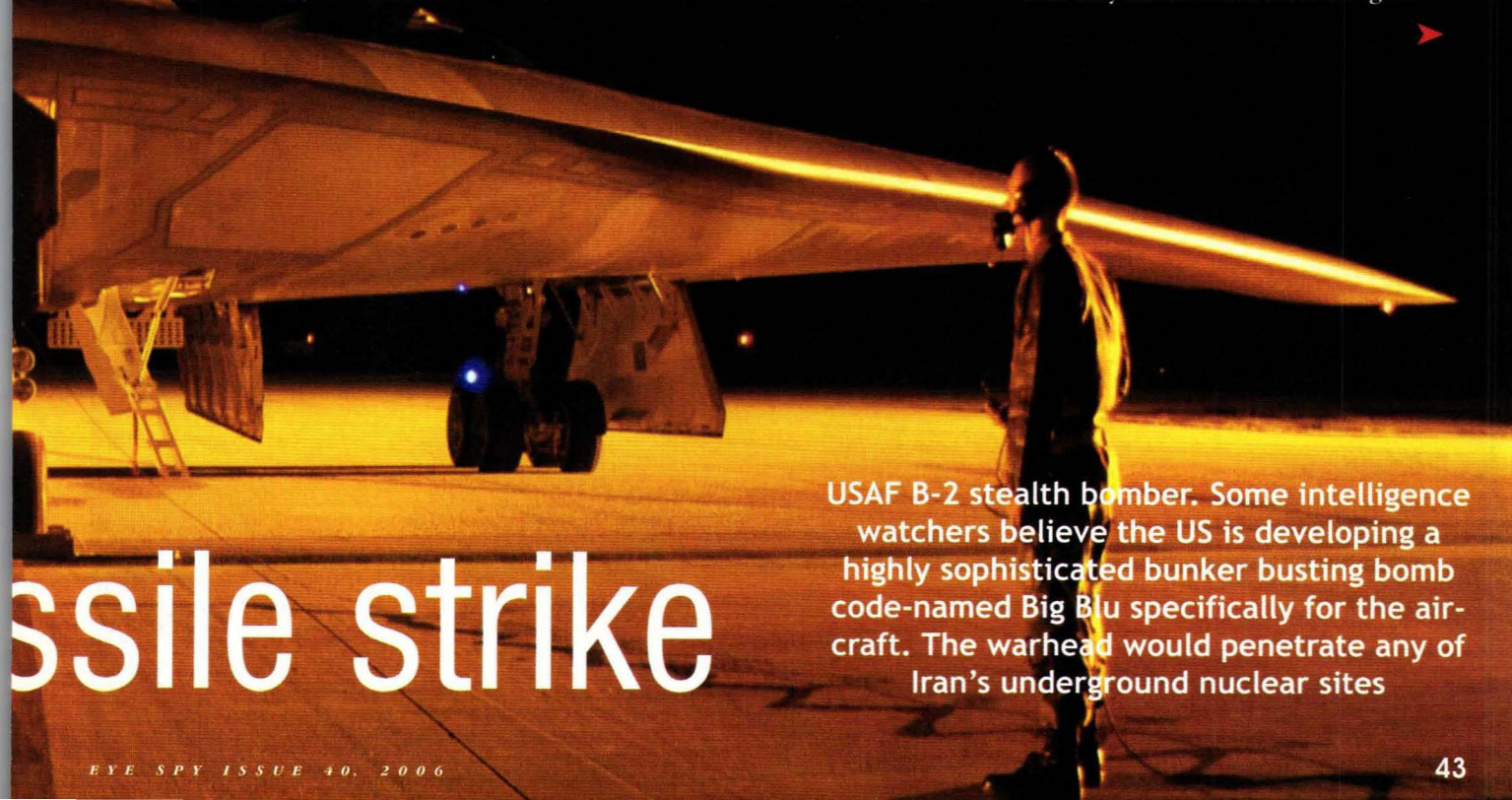
Iran's most powerful missile is the Shahab-3 missile, which can hit targets more than 2,000km from their launch site. Its Revolutionary Guard was equipped with the missiles in July 2003. "We are producing these missiles and don't need foreign technology for that," Safavi said. In 2005, Tehran also an-

nounced that it had developed solid-fuel technology for missiles. Analysts note that this affords the missile greater accuracy. The Pentagon has also established a special unit to monitor sales of Russian missile technology to Iran.

## MI6 AND CIA ACTIVITY

In a sideswipe at Britain and America, Safavi accused the US and British intelligence services of meddling in Iran, and in particular "provoking unrest in south-west Iran and providing bomb materials to Iranian dissidents." He claimed that both nations were

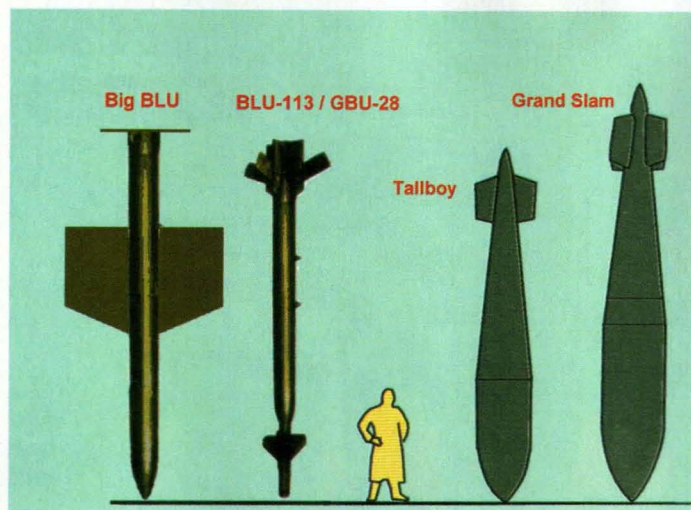
behind a series of blasts on 21 January that killed at least nine people in Ahvaz, near the southern border with Iraq. Some 9,000 British troops are based around Basra - just a few miles away. "Foreign forces based in Iraq, especially southern Iraq, direct Iranian agents and give them bomb materials," he said. Safavi warned that Iran's "intelligence people" were now monitoring dissidents and their supposed links with the US and British forces. "We are aware of their meetings in Kuwait and Iraq," he said. "We warn them [the US and Britain], especially the MI6 and CIA, that they refrain from interfering in



USAF B-2 stealth bomber. Some intelligence watchers believe the US is developing a highly sophisticated bunker busting bomb code-named Big Blu specifically for the aircraft. The warhead would penetrate any of Iran's underground nuclear sites

# ssile strike





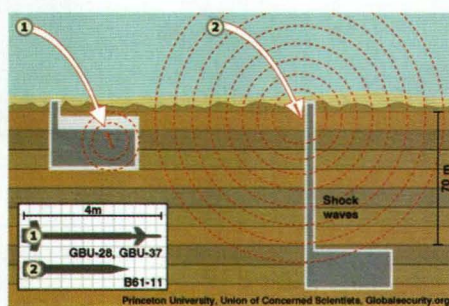
Iran's affairs." Whitehall sources dismissed the allegations as "daft."

### PROJECT BIG BLU

Over the last eighteen months the NSA and other agencies have been tasked with identifying Iran's secret nuclear sites. Intelligence analysts using highly sophisticated imaging satellites have 'mapped' hundreds of thousands of square miles seeking signs that covert nuclear facilities, not aligned to existing programmes, are being built. By analysing thousands of photographs, photo interpreters can pinpoint newly-built roads, buildings and all the infrastructure required to support research and development sites. One clue that usually betrays an on-going project is unusually heavy traffic and the laying of pipes and electricity cables. In remote areas, this is relatively easy. Satellites can track a single truck across vast distances and determine its exact position - night or day. And unlike the preamble to war in Iraq, and the known intelligence failures due to a lack of HUMINT (Human Intelligence), it is understood agencies like MI6 and the CIA are gathering vital information from reliable informants and agents.

Few military experts doubt NATO's or Israel's ability to hinder or thwart Iran's

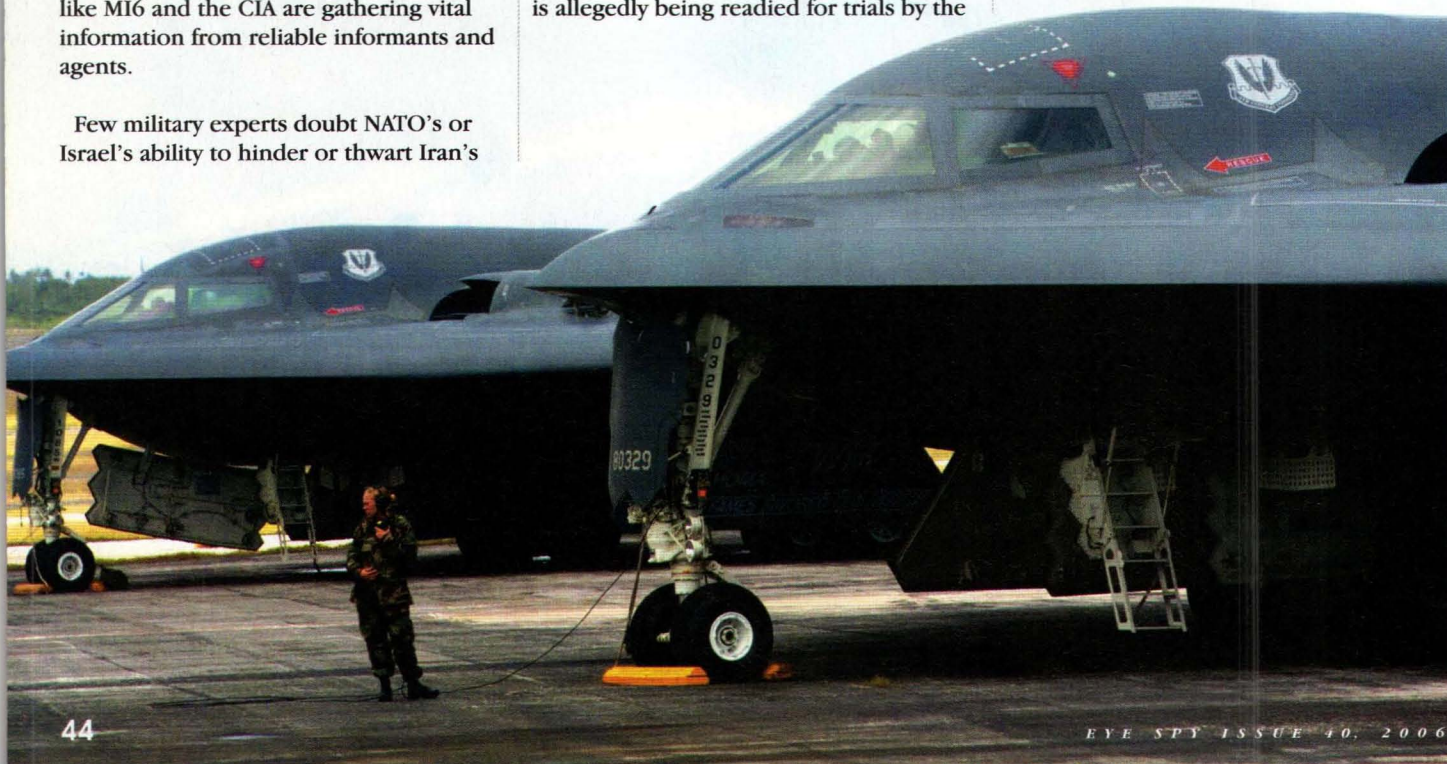
burgeoning nuclear programme. All, however, believe the ramifications for such action would be turmoil in the Middle East. While playing down the military option, behind the scenes military planners are being asked to consider the options for striking such targets. Since 1999, Iran has started building vast underground facilities in strategically placed positions that aircraft or missiles would find difficult to access.



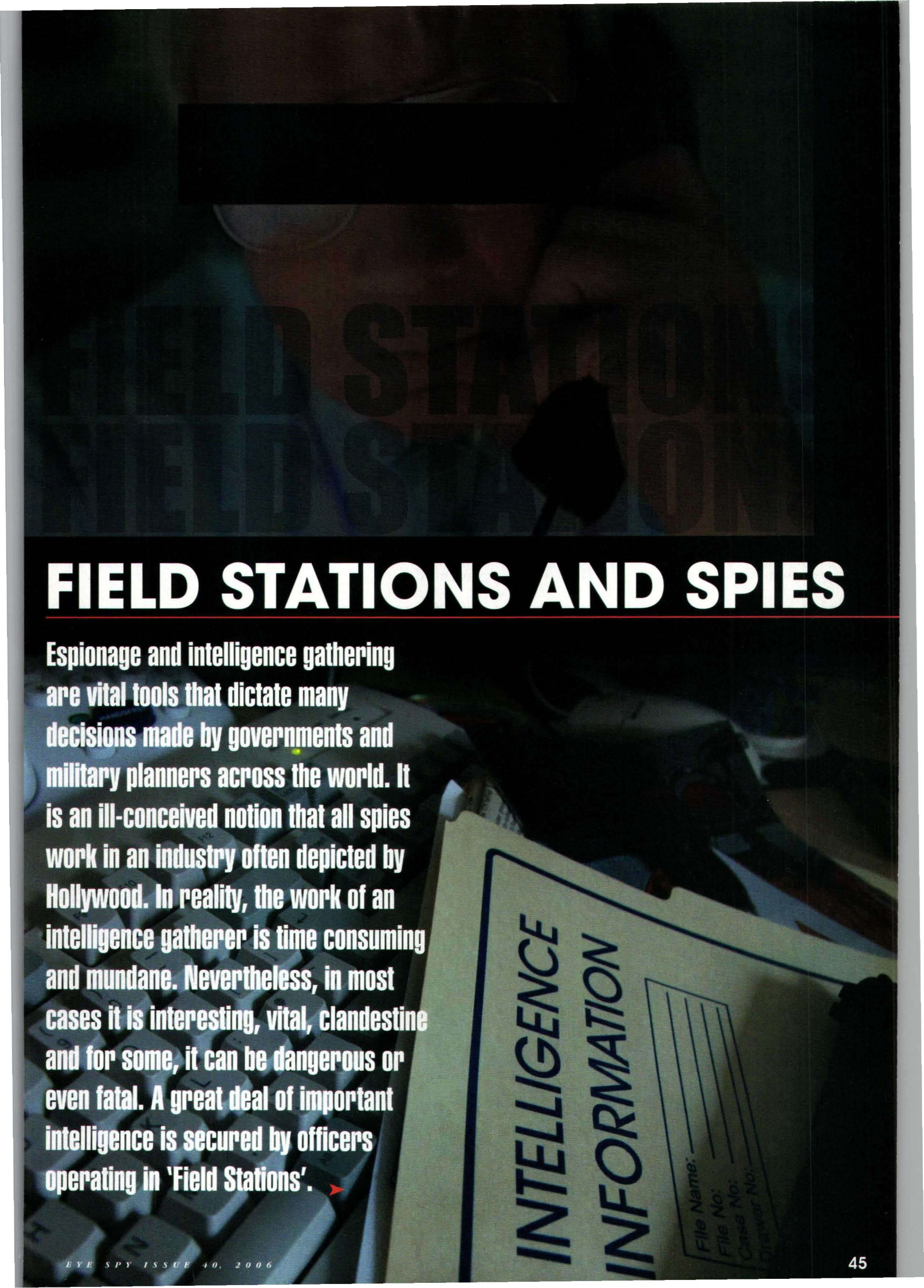
Even advanced 'bunker busting' bombs would be of limited use. With that in mind, news has emerged that a specially designed warhead - codenamed Big Blu - is allegedly being readied for trials by the

Pentagon. The 30,000lb bomb would be dropped by B-2 stealth bombers and guided to its target by advanced GPS. What makes this weapon far more deadly to underground sites, is its Cobalt-alloy body that allows it to penetrate an astonishing 150ft through solid rock. At this point the warhead is detonated igniting 6,000lbs of high explosives - enough to penetrate reinforced concrete hundreds of feet thick and disable sensitive equipment inside. There has even been talk of a limited nuclear strike using such bombs, but this is thought "highly unlikely".

Hardline Iranian President Ahmadinejad, who has called for the destruction of Israel on more than one occasion, insists Iran's nuclear programme is designed only for generating electricity. Officials in Russia have suggested that uranium for Iranian reactors could be prepared in Russia, a process that would in theory ensure that the fuel is not enriched to a level that would permit the material for military use.







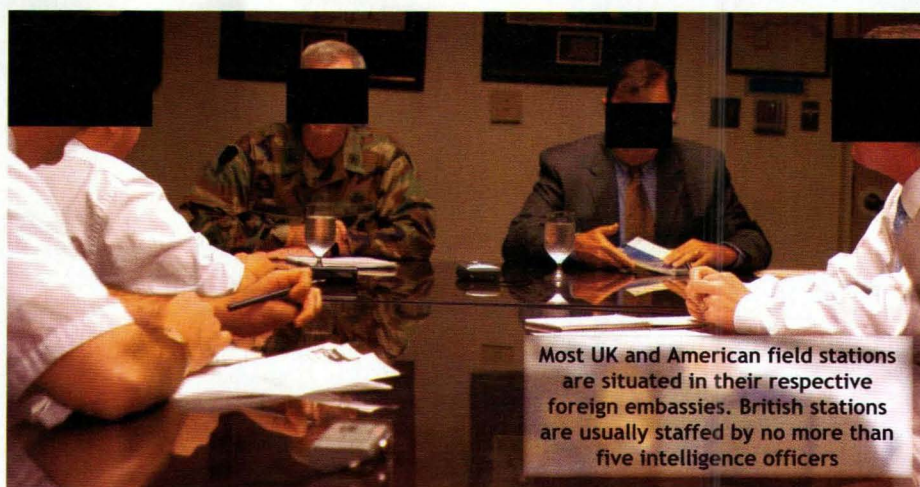
# FIELD STATIONS AND SPIES

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



**B**ritain and the United States both operate field stations under the watchful eye of MI6 (Secret Intelligence Service - SIS) and the Central Intelligence Agency (CIA) respectively. Obviously, station staff liaise and interact with other security bodies, including diplomatic and military officials. Other countries have similar concerns, the former KGB called its overseas stations "rezidenturas". The term 'field station' or 'station house' is somewhat confusing and has led to the misconception that the intelligence services have actual offices in situ - a "walk-in front door".

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



Most UK and American field stations are situated in their respective foreign embassies. British stations are usually staffed by no more than five intelligence officers

A station basically comprises of a number of officers assembled together who work on gathering and disseminating intelligence. It is their responsibility to understand, authenticate and quantify the data. In the case of MI6, the intelligence, sometimes referred to as "the product", is known as **CX**. This hails from the early days of MI6, its head 'C' in popular fiction, was Mansfield Cumming. These reports were regarded as top

secret and marked 'Cumming Exclusively', abbreviated to CX. Today, such reports are prepared and forwarded to senior officials in London (MI6 headquarters). The CIA produces its 'product' for analysis at Langley, Virginia (CIA headquarters).

A field station also acts as a conduit for secret intelligence requests. Most, though not all, are 'housed' in the

## FIELD STATIONS AN





relative safe environment of US or UK embassies (the CIA also has a number of domestic stations located throughout the United States). Working within an embassy compound provides additional security and privacy, not least because the building and personnel are protected under diplomatic law. Foreign security services are not permitted to enter the area unless permission is granted. In some environments that are considered safe, the station can be 'fronted' by a seemingly legitimate business.

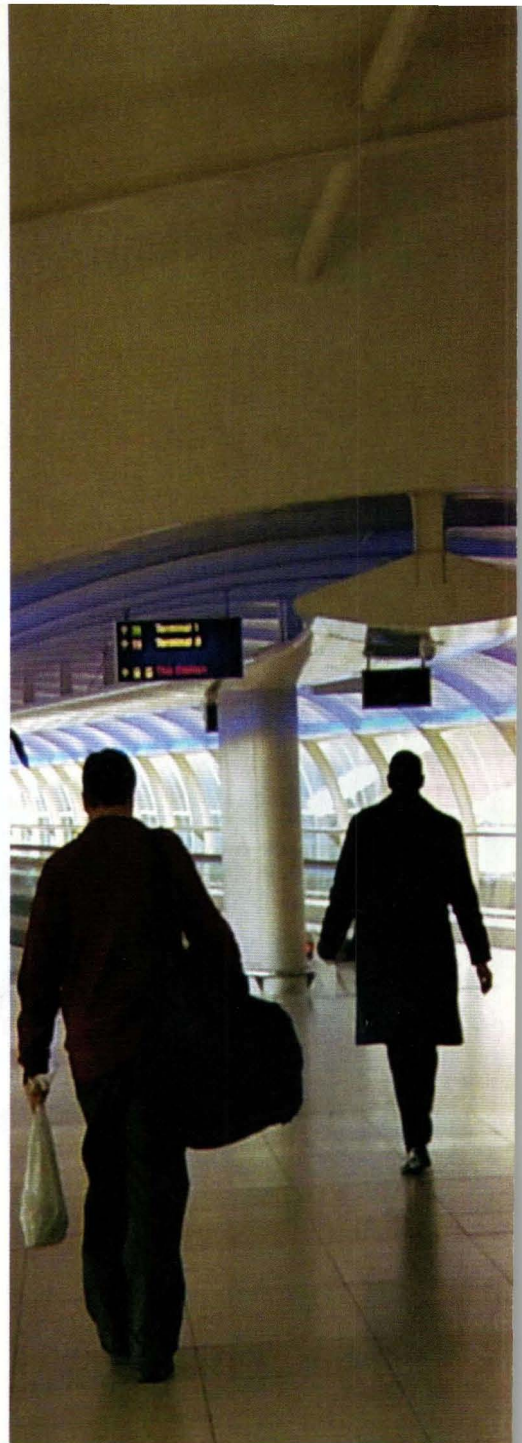
The size (personnel) of an MI6 field station is flexible and dependent upon various factors, including in-house diplomatic numbers, opportunities to gather intelligence, and the importance of the region. However, most stations are manned by about three or four intelligence officers from the intelligence branch (IB). MI6 has several hundred IB officers of which approximately half are deployed overseas and are based at field stations. In the case of Britain, most CX is gathered by these officers. Besides IB or field officers, the station is supported

where government relations are not good, or "trouble" lies just over the horizon. For those assigned to these stations, it is vital to acquire intelligence on the intentions of that nation, its partners and political agenda. However, both MI6 and CIA are alleged to have field stations that are manned by just one person - deep undercover and outside the protective shield that an embassy may provide.

#### INTELLIGENCE OFFICERS

A desk officer is often assigned to general security, intelligence analysis, administration and communications duties. Field, or case officers, are those chosen to obtain intelligence by using methods that invariably fall under the umbrella of espionage. Both play an important role in the running of a field station though could be separated by thousands of miles.

Besides administrative duties, a desk officer will occasionally support a field officer providing information, guidance and relating communications. However, one of his primary roles is to analyse intelligence. Much of the information landing on his or her desk is provided for using *open sources*. This could be from newspapers, television broadcasts, magazines, interviews, speeches by political leaders, academic studies etc. Sometimes the information looks like a mix of irrelevant facts that analysts refer to as *noise*. Experienced analysts can extract intelligence or signs that are of huge importance when merged with



## D SPIES

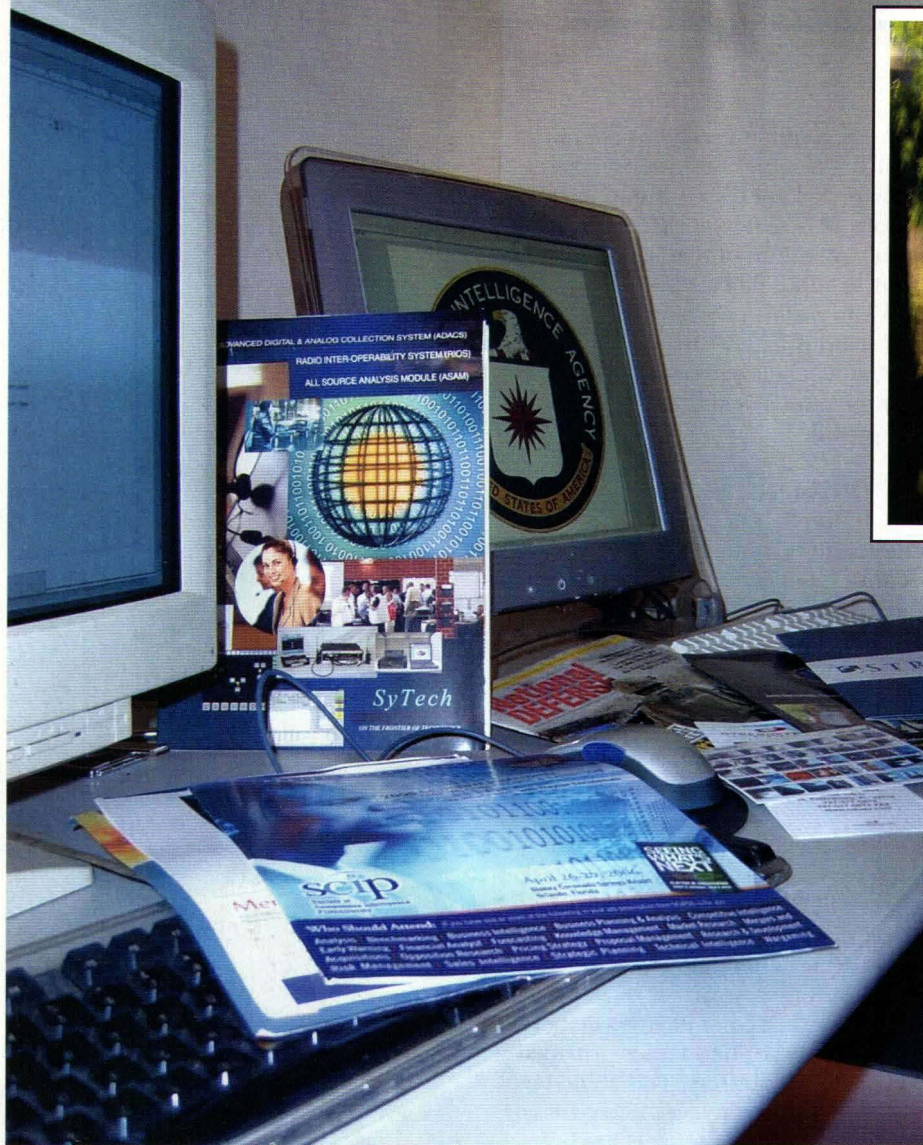
by one or two general service, or GS officers. Some larger stations cover areas (zones) which comprise of several countries. In times of conflict or heightened tension, it is not unusual to see additional 'specialist' persons joining a field station undercover in the guise of a diplomat. However, they are still vulnerable. Host governments can demand that named 'staff' be ejected. Usually, those asked to leave are suspected of espionage and may be field officers.

There are two types of station - *declared* and *undeclared*. A good example of a declared station is MI6, and its operation in Washington DC. Known to the intelligence community in the USA, MI6 cooperates closely with most services, but has a unique and working relationship with the CIA. Similarly, the CIA station in London is a declared 'entity'. In friendly countries, the head of the station is usually known to the host country, indeed, he will often make his presence known to draw attention away from his colleagues.

Undeclared stations often function in 'hostile' or potentially 'hostile environments' - *crisis areas*. For example, it is almost certain that intelligence gatherers will work under the guise of a diplomat







About 80-90% of all intelligence gathered by a field officer will be that from 'open source'. Intelligence not gleaned from open source has to be acquired by other means - and that usually means espionage

In many cases, and dependent on the political and military climate, field stations covering a particular country or region may be positioned outside the zone of interest. Others play unique roles. Following the invasion of Afghanistan by Soviet forces in 1979, a great deal of help was given to the Mujahedin by MI6 field officers in neighbouring Islamabad, Pakistan. Indeed, MI6 and CIA field officers helped coordinate resistance until the Soviets finally departed ten years later. MI6 has a major station in Vienna, Austria. Intelligence gathering here is aimed mainly at the Iranian and Russian communities, arms deals, and of course, just outside the city resides the important International Atomic Energy Agency.

other information. After assessing the data he will submit a report to the senior head of the field station for further action. He is sometimes referred to as *Station Chief*. If the data appears inconclusive or incomplete, the head of the station may approve more intelligence gathering, which often involves turning to the field officer. It is at this stage espionage may or may not be enabled.

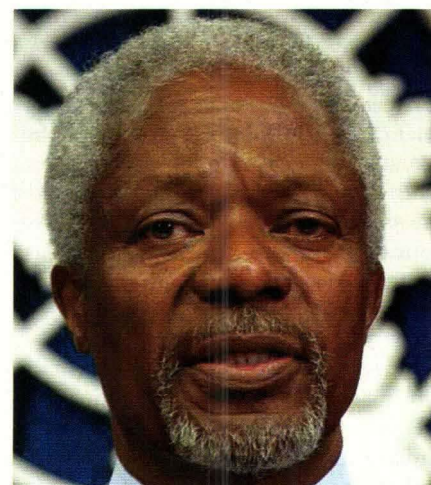
Undeclared stations are liable to receive a plethora of disinformation, be it from counter-espionage services (perhaps in the form of an anonymous letter), or a deliberate broadcast from a government-controlled television station. In hostile areas the disinformation flow can be aggressive and field station assessments become even more important.

Not all field officers are attached to a station. Occasionally officers are embedded with legitimate companies or provide peripheral support - warning against possible infiltration or a covert arms deal, for example. Their work could be so secret that the field station has no knowledge of the individual.

United States Embassy, London



The MI6 station in New York does not seek to obtain intelligence on America, but its primary role is to monitor and acquire data within the United Nations. Just prior to the second Iraq war, MI6 is said to have mounted a major spying operation inside the offices of several key personnel. This was done to try and determine voting positions on potential military action against Iraq. However,





wherever a field station is located, its role remains the same - intelligence gathering or conducting operations via a request.

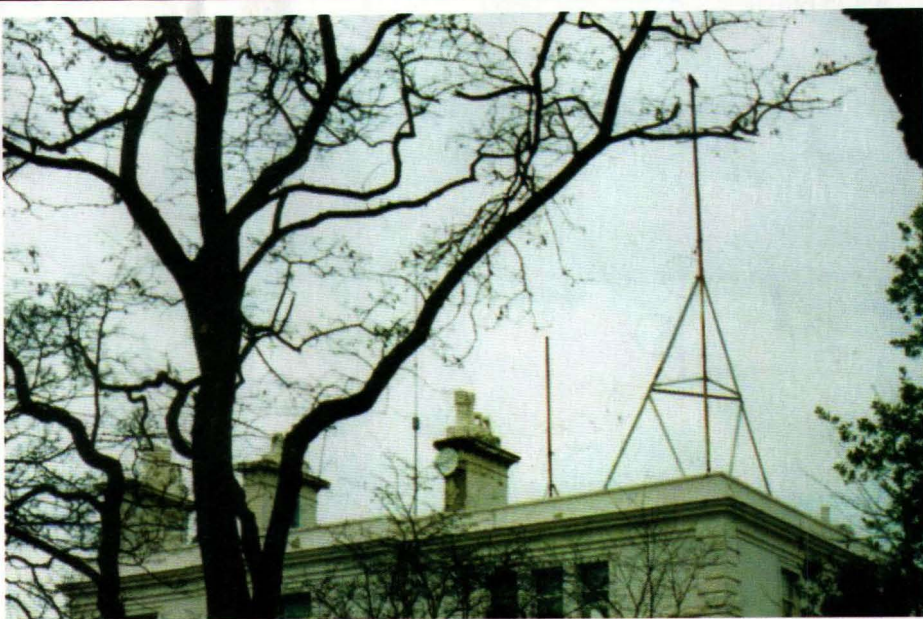
### THE FINAL JIGSAW PIECE

Open source intelligence can be supplemented by using three additional though clandestine methods. Field officers may use agents (HUMINT - human intelligence), electronic measures or seek the help of friendly intelligence agencies. The outcome is always the same - the file is eventually forwarded to London or Washington for action. Transmitting intelligence by electronic means from the station to headquarters is important. Each embassy-based station has a highly secure communication route. Only intelligence staff have access to the transmitting rooms. These rooms are 'swept' regularly for listening devices, and are constantly monitored for breaches in security.

Both MI6 and the CIA have hundreds of field officers deployed around the world.



MI6 is alleged to have bugged the offices of UN General Secretary, Kofi Annan and other officials. Critics say the operation was performed via its New York field office



Communications equipment atop of Russian Embassy in London. Like MI6 and the CIA, Moscow has its own spies. Recent estimates put the number of Russian spies operating under the guise of diplomats (below) and businessmen in London at 100



Since 9/11, their numbers have increased dramatically and, in recent times, a number have been assigned to augment covert military units. Wherever a field officer is sent, he or she is expected to be able to speak the native language and have a good grasp of knowledge about the host country.

There has been criticism within the intelligence services that both services are "thin on the ground" in some conflict areas. For instance, prior to the invasion of Iraq, the CIA had no covert presence in the country, MI6 had but one or two officers. Intelligence was often provided for by foreign agencies and invariably this was incomplete.

It is unlikely a field officer will 'actively' participate in major espionage operations, though it can happen. Recent

events in Moscow involving MI6 and its 'spy rock' come to mind (see Eye Spy 39). In most cases, the officer will try and create a network of 'volunteers' to help obtain intelligence.

### PROFILING AND CULTIVATION

Both Britain and America have created excellent training programmes whereby field officers can use their skills to actually manufacture or select the "right agent". Identifying possible agents is called *profiling* - it's a tricky and very dangerous task. If the "wrong" person is chosen it could compromise the real identity and role of the field officer. Once a target has been identified, profiling specialists are used to check their background to determine if the subject is suitable. If the station chief



## 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](http://www.lepl.co.uk) email: [leplinfo@aol.com](mailto:leplinfo@aol.com)



green lights the move, then *cultivation*, as it is called, takes place.

Foreign citizens may volunteer information; their motive is sometimes altruistic and even patriotic. Of course, some agencies may resort to using money, blackmail or honeytraps to convince foreign citizens to betray their country. Even after a subject has been turned, field officers must constantly assess the accuracy of the information that he or she is submitting. *Walk-ins* are persons who are not recruited but instead offer their services. Occasionally such persons are actually counter-intelligence officers trying to infiltrate field stations. A series of tests and measures have been developed to expose persons posing as potential *information volunteers*. Naturally, field officers are on high alert and deeply suspicious.

However, in most cases field officers are grateful for persons supplying intelligence freely. Dubbed a *defector in place* these *human assets* have supplied vital information that could not have been obtained by technical means. This does not mean the data could be false. Intelligence on Saddam's weapons of mass destruction was submitted by such a person to MI6 and the CIA.



It turned out to be woefully wrong. Interestingly, the head of the station does not expect field officers to identify their agent, or intelligence asset. His or her life could depend on the officer and any

A field station within an embassy will have its own secure communications and committee/conference room



Intelligence is forwarded to MI6 headquarters London by some 50 field stations



disclosure of this information could prove fatal.

#### ELECTRONIC INTELLIGENCE GATHERING

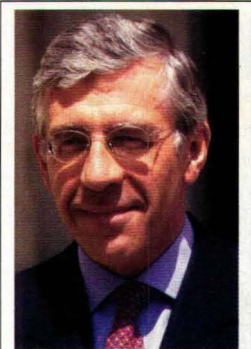
Since the end of the Cold War, the CIA has become very reliant on the National Security Agency for electronic intelligence gathering. Prior to that, the agency's Science and Technology Directorate used a wide variety of electronic techniques to gather intelligence, including planting

listening devices, intercepting radio transmissions, and using seismic sensors and satellites to monitor military activity around the world - the agency even had its own 'listening field stations'. Yet, senior intelligence officials recognise that none of the above can replace or command as much importance as HUMINT. Field officers still have to be conversant with many of the old eavesdropping methods, though actually placing bugs in buildings, vehicles and on people, is usually carried out by 'volunteers'. Since the outbreak of hostilities in Iraq, the CIA and MI6 have begun programmes to increase their HUMINT capabilities. The CIA recognised that its intelligence gathering potential was weak and decided to increase its number of field officers.

Though embassies are 'protected' by international law, terrorism is now a primary concern, and concealing the identity of intelligence officers is paramount to their well-being. In 2006, a Greek media outlet actually "outed" the identity of a number of MI6 officers. This followed reports that MI6 had participated in the interviewing of a number of people in Greece, just days after the July London terrorist attacks. The communist newspaper, *Proto Thema* named a British official as the MI6 station chief in Athens. A few days later it published a photograph of the officer jogging on the streets of Athens. Britain vehemently denied the allegations, but the officers were still withdrawn. A few months later, Russia's FSB published the identity of alleged MI6 field officers participating in covert communications with non-governmental

organisations. The officers usefulness was diminished.

While none of the men's lives were threatened, the incidents were of major embarrassment to MI6. However, attacks against field officers do occur. In 1983, a suicide bomber in Beirut devastated the US embassy and killed sixty-three people, including all six members of the CIA's field station. Visiting at the time was a legendary CIA field officer with long experience in the Middle East, Robert Ames, whose death was confirmed by the wedding ring on a hand retrieved from the debris. His replacement was later kidnapped and killed.



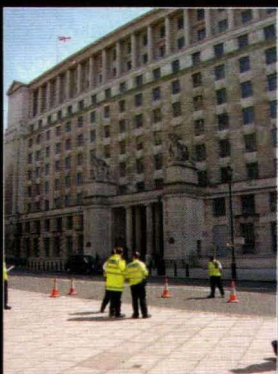
Foreign Secretary Jack Straw, whose department oversees MI6, rejected Greek media claims. MI6 has no official spokesman

#### DEDICATED STATIONS

Occasionally special dedicated 'stations' are created to tackle specific problems. Prior to the attacks of 9/11 the CIA initiated a plan to quicken the flow of intelligence on Osama bin-Laden and al-Qaida - the Bin Laden-dedicated Issue Station. A government note on the Counter-terrorist Center's (CTC's) offensive operations stated: 'This Station, staffed with CIA, FBI, DOD, and NSA officers, has succeeded in identifying assets and members of Bin Laden's organisation, and nearly 700 intelligence reports have been disseminated about his operations'. Unfortunately it wasn't enough to thwart the attack.

Policymakers in London and Washington DC are often guided by intelligence gleaned by field officers, or the analysis of an officer. The intelligence that may start as a single line statement in an obscure journal, or a tip about a potential terrorist could be instrumental in forming military or economic policy for years to come. It may also prove to be vital in determining the opponents true intention, be it benevolent or otherwise.

A major decision affecting everyone can have its genesis on the desk of a field officer working in a remote land. It's worth remembering this the next time you read a newspaper report about Iran's nuclear ambitions... or intent.



Intelligence acquired by CIA and MI6 is often requested by 'users'. Two primary users are the Ministry of Defence (above), and the US Department of Defense





# TRICKS OF THE TRADE SPYCRAFT

Undertaking surveillance of a target, vehicle or location can be a time consuming business. It can also prove expensive. However, if an operation simply entails finding out what time a vehicle was driven away, then there is a very inexpensive method that is almost always successful - it's called the 'watch trick'.

Besides being applied to covert surveillance, the trick can provide lots of interesting data. Managers can monitor the length of time a person attends a business meeting or the hours worked in a shift - just in case an employee starts to add a few hours to his time sheet. Suspicious spouses can discover just how long their partner has spent at a specific location. Undoubtedly readers can add to this list.



Don't let anyone see you place the watch under the tyre - or recover the watch

To perform this 'time old' 'off-site' surveillance trick, you must first obtain a watch, scissors and tape [1]. There are few rules here, suffice to say the watch must use hands (old wind-up type) and be fully functioning before it is placed into position. This trick will not work with a digital quartz watch. Similarly, we would not advise using an expensive time piece! A second or third-hand watch usually works just as well as a new one. These can be purchased in second-hand shops, in markets or increasingly at 'car boot' meetings. They normally cost between two or three pounds or \$5.00. Before the trick is applied, test the watch for a few days to determine if it is functioning properly, to make sure it is not losing or gaining time, or more importantly, does not work at all. It makes little or no difference if the face is plastic or glass, however, we found that the depth, or 'bowl' of the glass is very important. If the depth of the face is thin, then the vehicle's tyre may not break the glass.

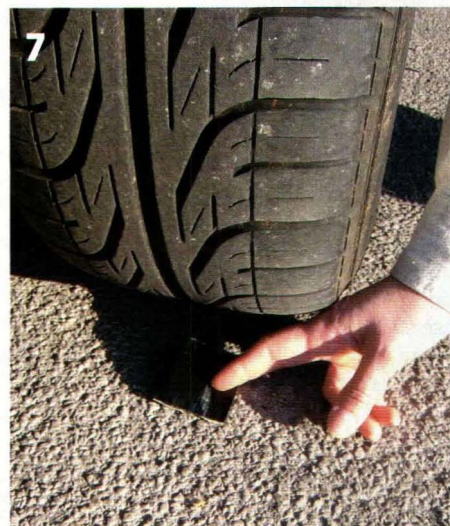
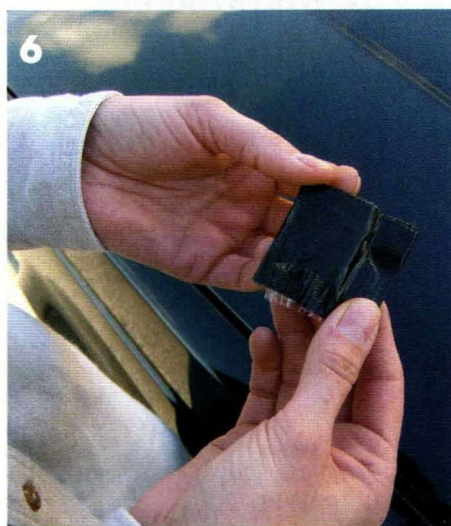
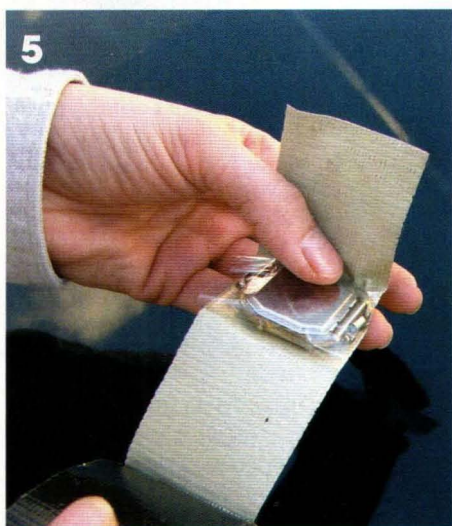
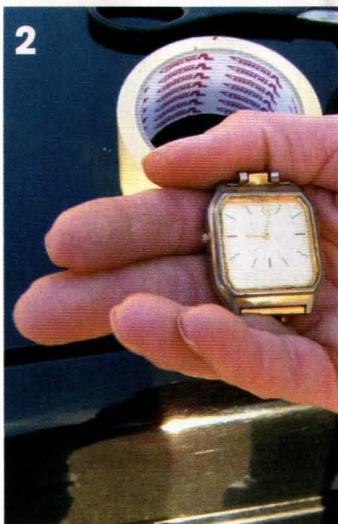
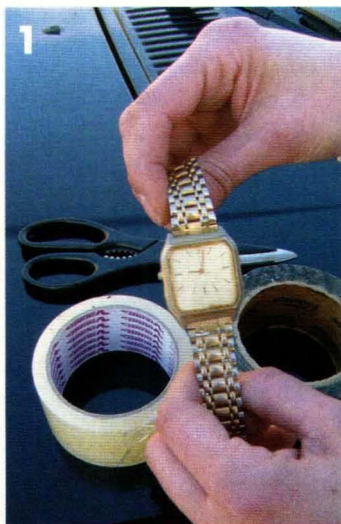
Your first task is to remove the straps leaving only the actual watch [2]. Then take a wide strip of sellotape and carefully cover the face and fix to the rear of the watch [3 & 4]. The rear of the watch can be painted grey or black (to merge into the road colour) though this is not



The trick will work in many environments - including car parks

# The Watch Trick





necessary. A piece of dark cloth or tape (black electrical tape is excellent) is then wrapped tightly around the watch [5 & 6]. Using both clear and electrical tape will help protect the watch from rain, snow, frost etc.

Some intelligence experts advise the watch should be tucked in front of the tyre opposite the driver's side. This is primarily because once the vehicle has been driven away, it will remain close to the pavement enabling its recovery. Also, it is unlikely the driver will

notice the object when they get in the vehicle. However, because the object is so small, it is unlikely to be discovered under any tyre [7].

When the vehicle is moved, the tyre crushes and breaks the watch. The sellotape (or similar) should hold the watch hands in place, while the tape or cloth will help conceal it from passers-by [8].

Retrieve the watch and carefully remove the outer tape or cloth. The hands of the watch will

be fixed at the very moment the mechanism failed and reveal what time the vehicle was moved [9].

In the event you simply want to determine if a vehicle has been used since the last time it was under observance, any paper or plastic drinks carton can be placed under the tyre. Operators can also use plastic tomato or mustard condiments available from most fast food outlets such as McDonald's etc. If the packet has been burst, the vehicle has been moved.







## EYE SPY ON- LINE

CHECK OUT OUR MASSIVE NEW  
RANGE OF SURVEILLANCE  
PRODUCTS AT

[www.eyespymag.com](http://www.eyespymag.com)

### HOMEGUARD VIDEO CAPTURE UNIT

The only battery operated security camera recorder with portability in mind that fits in your pocket. It has a built in high-resolution colour camera and a recorder to provide flexible application use. Built-in OSD (On-Screen-Display) for easy setup, featuring all the basic functions found in professional DVR recorders. The unit takes fast action snapshots when motion is detected. Simply place the unit where you wish to capture video and it will automatically record fast-action snapshots. Playback on your own TV, and save recordings to your VCR, it's that simple! It is capable of capturing more than 16000 frames. Easy and discrete to use, this new item is perfect for home, office or anywhere you need personal protection.

Put it in your pocket for portable  
surveillance purposes. Place the compact unit  
on the dashboard of a vehicle for outdoor  
event recording

### EYE SPY READER OFFER



#### FEATURES

- Very User-Friendly
- NTSC/PAL
- Portable & Compact
- Built-in 64MB Flash Memory
- Built-in Hi-Resolution • Pinhole Colour Camera
- Continuous or Motion • Detection Recording
- Adjustable Motion/Detection Sensitivity Level
- Image Quality Recording [VGA (640x480) QVGA (320x240)]
- Three-Level Compression Quality High, Medium, Low
- Date & Time Stamp
- DC 12V or 4 x AA batteries
- 6 Hours Continuous Recording



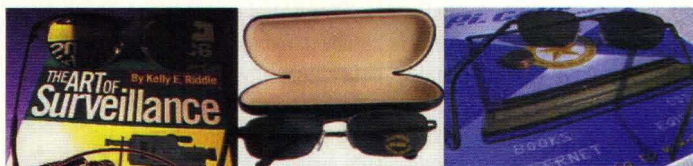
REGULAR PRICE: £425.00 \$295.00

NEW PRICE - LIMITED TIME OFFER UK £295.00 USA \$260.00 ROW: £305.00

Order code: ES/HOMEGUARD

## SURVEILLANCE ACCESSORIES

### REAR VISION SURVEILLANCE SUNGLASSES - NEW DESIGN



Ideal for Overt, Covert and Countermeasures

These high quality sunglasses look like regular sunglasses with one unique exception. They are a little wider on the ends and have mirrored edges on the inside of them so you can actually see behind you while you are looking forward. Don't confuse these sunglasses with cheap toy models. This model is used by professional law enforcement agencies throughout the United States and elsewhere.

Order code: TX-RVS UK £30.00 USA \$31.00 ROW \$35.00

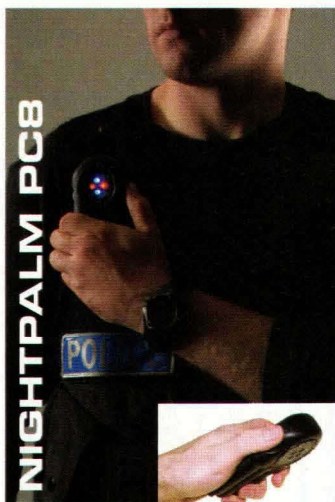
### CELL PHONE MICROPHONE

This new microphone/earphone allows you to record conversations made from and to your cell phone when connected to a recorder. Simply insert the plug of the cell microphone into the mike jack of your tape recorder and insert the mike pickup (with foam pad) into your ear. Set your tape recorder in the 'record' mode and both conversations are clearly recorded. Now you can eliminate the danger of trying to write messages, orders or directions while driving. Simply tape them and play them back later. No need to fumble around looking for a pen and paper! The compact design of this earphone microphone allows you to record all calls.



Specifications 3.5 mm input jack- 2.5 mm input jack (included) - Weight - 12 grams

Order code: TX-CPM UK £69.00 USA \$83.00 ROW £70.00



NIGHTPALM PC8

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.eyespymag.com](http://www.eyespymag.com) or our free equipment catalogue

Order code: PC8 Police  
UK £40.00 USA \$85.00  
ROW £45.00

Order code: PC8 Outdoor  
UK £40.00 USA \$85.00  
ROW £45.00

### New Generation COUNTERTEK RF ADVANCED DETECTOR



#### COUNTER-MEASURES - BUG DETECTOR

Provides a wide sweeping range from 50 MHz to 3 GHz. Adjustable digital sensitivity display with nine LED lights. CounterTek comes with a rechargeable battery and power cord, earphone jack for silent operation and vibration mode.

Measures just five inches 5 x 2.5 x 0.5 inches

UK £210.00 USA \$300.00

ROW: £225.00

Order code: ES/COUNTERTEK

### WIRETAPTEK TELEPHONE TAP DEFEAT



Designed to automatically detect and disable most forms of wire taping and telephone bugging.

Equipped with an LCD voltage meter to monitor phone line conditions. A red LED will flash at the possibility of wire tapping on the line and conversation will be automatically cut off by the Super Tap Buster to prevent your voice from being heard or recorded.

When the 'beep' switch is set to the ON position, a continuous warning 'beep' will be transmitted to the person on the other end indicating that the conversation has been cut off due to wire tapping or telephone bugging.

UK £155.00 USA \$199.00  
ROW: £170.00

Order code: TX/WIRETEK



# THE WORLD'S SMALLEST RECORDERS

## EYE SPY EDIC

18.6-HOUR DIGITAL AUDIO RECORDER

Law enforcement grade, the size of a paper clip/push pin. You can completely palm this and wrap your hand around it. Amazing 18.6 hours recording time.

- Dimensions: 34 x 25 x 7mm
- Weight: 8 Grams
- Built-in FLASH memory
- Voice storage capacity: 18.6 hours
- Power source: Battery CR2032
- Battery life in record mode: 17 hours
- Battery life stand-by mode: Three months



UK £350.00 USA \$725.00  
ROW: £365.00  
Order code: TX-EDIC



EDIC TELEPHONE RECORDING ADAPTOR £35.00/\$55.95

## THE AUDIO MICRO DOT

37-HOUR DIGITAL AUDIO RECORDER

The world's smallest, high grade law enforcement/broadcast micro digital audio recorder.

- Dimensions: 40mm
- Weight: 15 Grams
- Memory: 256MB for 37 hours of recording time
- Power source: Battery lithium CR2450
- Battery life in record mode: 60-70 hours
- Battery life in stand-by mode: Three months two weeks



UK £400.00 USA \$800.00  
ROW: £415.00  
Order code: TX-AMD



MICRO DOT TELEPHONE  
RECORDING ADAPTOR  
£35.00/\$55.95

## EYE SPY SEED MICROPHONE



This seed microphone is so small it can be used in a variety of ways - hide in a car, under door, bag, sleeve anywhere. 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



An ordinary pen with a difference! Contained inside 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

## EARPHONE VIDEO CAMERA

Wired video camera built into an earphone. Use with a pocket-sized digital video recorder for a self contained covert video recording system. High grade CCD camera uses 1 9V battery.

Order Code: TX-EARVIDCAM  
UK £270.00  
USA \$395.00 ROW £285.00



## DNA100 4.3" Portable Navigation System

Multifunctional GPS mapping system with MP3/MPEG-4 playback. Turn-by-turn voice guidance with door to door navigation. Includes cigarette lighter adaptor, window mount kit, cable mount, USB connector and neck strap.

Currently available only to  
US and Canadian readers



USA \$545.00 (UK please enquire) Order code: TX-DNA100

## 4.3" PORTABLE NAVIGATION DNA-100

MP3/MPEG-4 playback  
Reliable O/S(Windows CE Netscape 4.2)  
4.3" Wide TFT LCD and touch screen  
Built-in Li-polymer(2500mAh)over 4h under MPEG-4  
Voice guidance  
SD/MMC/USB HOST 1.1  
FM transmitter(optional)  
DVB-T/H, DMB receiver(optional)

## REVERSE PEEPHOLE VIEWER - Used by Law Enforcement



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 £130.00 USA \$159.50 ROW £140.00



Please write for our free 32-page  
catalogue of specialist surveillance  
equipment, or visit  
[www.eyespy.com](http://www.eyespy.com) to view  
our huge range



0800 122 522

Welcome to  
**access**  
storage solutions

Police raid the  
storage unit  
near Heathrow  
Airport in  
March 2004



# Operation Crevis

## 'THE BRITISH BOMB PLOT'

**M**uhammad Babar, a terrorist-turned-informant, said he conspired with several followers of Osama bin-Laden to attack numerous targets throughout the UK. Flown into London with a US Marshal escort, Babar has been giving evidence at the Old Bailey Court.

On 30 March 2004, British anti-terrorist officers supported by various personnel launched Operation Crevis. Several addresses in and around London were raided, including an Access storage facility close to Heathrow Airport. Inside the unit, officers discovered a huge amount of ammonium nitrate fertiliser. Unbeknown to the media, MI5 and the FBI had been conducting a major intelligence operation months prior to the raid, gathering information from across the globe on

those suspected of targeting the UK. GCHQ had also intercepted numerous calls that suggested an attack was imminent. Operation Crevis involved 700 police and support staff.

Babar, 31, had travelled from his home in the United States just days after 9/11 to fight with al-Qaida followers in Pakistan - despite the fact that his mother, who worked in the World Trade Center, had narrowly escaped death when the hijacked airliners struck.

### FBI informer reveals al-Qaida's British targets

Dubbed the "American supergrass" by the media, Babar has already admitted that he had plotted to kill the Pakistani president.

He told the court about his role in two failed assassination attempts against General Pervez Musharraf in 2002. He also acknowledges that he would be facing the death penalty in Pakistan, had he not done a deal with the FBI. Speaking with an American accent, Babar explained he had helped one set of would-be assassins obtain AK47 firearms, ammunition and grenades.

He said none of the seven men on trial at the Old Bailey had anything to do with the Pakistan conspiracies.

Babar is giving evidence against six of seven defendants arrested as a result





of Operation Crevis. They are standing trial for conspiring to cause an explosion in Britain. He alleges that 'cell members' discussed striking

numerous targets, including a shopping centre, a London nightclub, railway stations and Britain's power and transport infrastructure. The attacks would take place simultaneously or in close succession. Other proposed operations allegedly included poisoning beer for sale at British football matches and setting up mobile hamburger vans and poisoning the food before handing it over.

Babar has already pleaded guilty in New York to various terrorist-related offences, and told FBI investigators about the "British bomb plot". He is the first supergrass linked to al-Qaida to give evidence in a Western court and has been given immunity from prosecution in relation to his evidence in the UK. When he was first interviewed he denied any wrong doing but later said: "I knew what

I was involved in and I knew there was a paper trail behind me as far as emails and money transfers [were concerned]."

Intelligence sources linked Babar to an al-Qaida bomb plot that involved acquiring a large amount of ammonium nitrate fertiliser and aluminium powder, which the prosecution alleges were components for explosives to be used in attacks in Britain. Babar admitted providing "material support" including computers to at least one suspect. The jury was told that his involvement related to his expertise in explosives and acquiring bomb parts.

Babar denied suggestions from Joel Bennathan, counsel for Omar Khyam, one of the seven defendants, that his evidence against Mr Khyam was not true and that he had taken speculation and "twisted it into a firm and settled plot in the UK" to make himself a valuable witness.

The seven men accused of being part of the terror cell deny conspiring to cause explosions likely to endanger life between 1 January 2003 and 31 March 2004. Two others also deny a charge under the Terrorism Act of possessing 600kg of ammonium nitrate fertiliser for terrorism. The trial continues.

## Moussaoui Sentenced to Life in Prison

**ALEXANDRIA:** A US federal judge sentenced al-Qaida conspirator Zacharias

Moussaoui to life in prison for his role in the September 2001 terror attacks. Judge Leonie Brinkema handed down the sentence after a 12-member jury rejected the government's argument for execution. The life sentence comes without any possibility of release.



US District Judge Leonie Brinkema sent Zacarias Moussaoui to prison for life to "die with a whimper," for his role in the terrorist attacks. He responded: "God save Osama bin Laden - you will never get him."

Brinkema firmly refused to be interrupted by Moussaoui as she disputed his claim that his life sentence meant America had lost and he had won. "Mr Moussaoui, when this proceeding is over, everyone else in this room will leave to see the sun... hear the birds ... and they can associate with whomever they want," she said. "You will spend the rest of your life in prison."

The 37-year-old convict, a French citizen born in Morocco, is expected to spend the rest of his life in what is called a 'super-maximum security' prison in the western state of Colorado.



Left: Former Metropolitan Police Commissioner Sir John Stevens headed Operation Crevis. Above: The suspects are driven to the Old Bailey Court



# The Public Heroes

The 'legend of Flight 93' is very real indeed. What still cannot be determined is if the passengers actually forced their way into the cockpit...

## of United Airlines FLIGHT 93

**U**nited Airlines Flight 93, one of four aeroplanes hijacked on the morning of 11 September 2001, crashed in a Pennsylvania field about 30 minutes after it had taken off from Newark. Thirty-three passengers and seven crew members died, along with four terrorists. The exact circumstances of how the Boeing 757 fell out the sky has been a relatively guarded secret. However, it has always been suspected that the remarkable bravery of ordinary men and women - some who tried to overpower weapon-wielding hijackers - was to blame. This has been disputed by some analysts, but following the release of audio tapes at the trial of Zacarias Moussaoui in a federal court in Alexandria, few would doubt that at the

very least their heroic action unnerved the terrorists and forced them to abandon their mission to destroy either the Capitol Building, or even The White House.

Prosecutors played the tapes in an effort to reveal the terrifying last moments of Flight 93. Government lawyers believe that had Moussaoui, the suspected '20th hijacker' told investigators what he knew about the plans, the 9/11 attacks could have been thwarted. Earlier, the court had heard several final phone calls to and from loved ones as the World Trade Center was destroyed.

The Flight 93 tapes began with a hijacker's voice: "Ladies and gentlemen, this is the captain ... we have a bomb on board, so sit." Moments later desperate

pleas from an attendant or crew member are played. The jury heard blow after blow reigning down on the unidentified person. "Please, please don't hurt me," the voice said... "I don't want to die." Silence followed and the hijacker cried "That's it... everything is fine. I finished." The person had been killed.

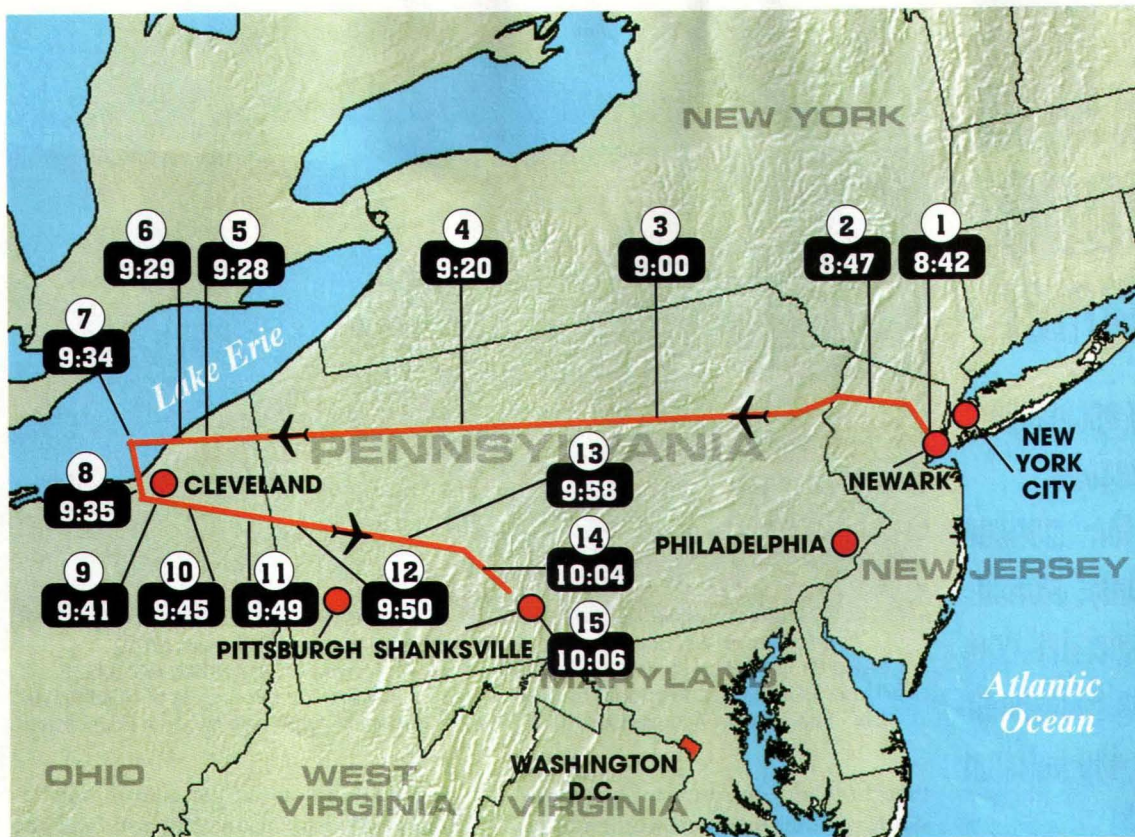
Radar tapes in correlation with the cockpit recorder, show that at that precise moment, Flight 93 banked left



Zacarias Moussaoui - claims he was not part of 9/11 conspiracy but was involved with 'second wave'

## Remarkable courage of hijacked passengers finally acknowledged as cockpit tapes released to public





## APPROXIMATE TIMELINE

1. United Airlines Flight 93 departs Newark International Airport
2. Altitude 10,000ft
3. Altitude 31,000ft. UA warn all pilots of possible security breaches and to take precautions to barricade cockpit doors
4. Hijacking begins. Passenger Tom Burnett calls his wife to explain incident
5. Tape in cockpit reveals someone shouts "get out of here!"
6. Passenger Jeremy Glick calls his wife and described the hijackers. Mrs Glick explains New York has been attacked
7. A hijacker announces there is a bomb on board and the aeroplane is returning to the airport
8. Flight 93 begins to turn near Cleveland
9. Passenger Marion Britton telephones friend explaining two passengers have been killed
10. Tom Burnett's phone is transferred to Verizon cell phone operator Lisa Jefferson. He explains that passengers have a plan to take back the aircraft
11. Pittsburgh Airport Flight Control Tower staff evacuate building fearing Flight 93 will be crashed into airport
12. Passenger Sandra Bradshaw calls her husband saying they are filling cups with hot water to use against hijackers
13. Passengers try and force their way into cockpit. Confrontation with hijackers now occurring. Hijackers respond by violently moving wings
14. Johnstown-Cambria County Airport log: Flight 93 is 15 miles away - speed increasing
15. Witnesses on ground see aircraft flying low & erratically - seconds later Flight 93 crashes near Shanksville - eighty miles from Pittsburgh

towards Washington DC. What followed has already been recognised by intelligence officials as a pivotal moment in hijacking history. No longer can hijackers expect passengers and crew to remain simply obedient and transfixed by terror.

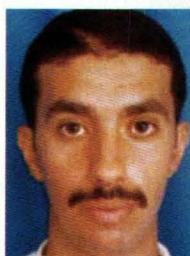
The 32-minute tape is fragmented and difficult to hear. Voices in English and Arabic are often inaudible. Nevertheless, it is representative of an epic struggle. Passengers can be heard openly discussing how to retake the

airliner, using whatever weapons they could find. "Let's get them!" a passenger shouted as dinner plates crashed to the floor. "In the cockpit... if we don't we'll die!" said another. For those critics and commentators who had previously rejected the theory that the passengers fought back, this was a 'bitter pill' to swallow. The 'legend of Flight 93' is very real indeed. What still cannot be determined is if the passengers actually forced their way into the cockpit. However, they were certainly at the

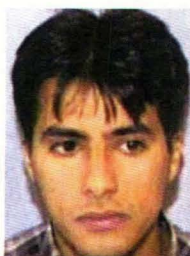
## THE HIJACKERS



Saeed Alghamdi



Al Haznawi



Ahmed Alnami



Samir Jarrah

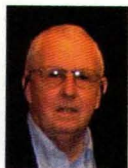


Government photo showing part of United Airlines Flight 93 following crash

Continued on page 82



# Letter from Fort Meade by David Hamer



...being an irregularly occasional, or an occasionally irregular, communication from the American cryptological community: particularly those things associated with the National Cryptologic Museum [NCM] and its parent, the National Security Agency [NSA]

## NEW FOR EYE SPY



**T**o quote from an official history: "The National Security Agency was created in November 1952 and has provided timely information to US decision makers and military leaders for more than 50 years. However, even before President Truman signed the memorandum establishing the Agency, pioneer cryptologists laid the groundwork for an organization that would play a critical role in the outcome of all major conflicts. Cryptologist legends such as William and Elizebeth Friedman, Frank Rowlett, Agnes Meyer Driscoll and Herbert O. Yardley are remembered for

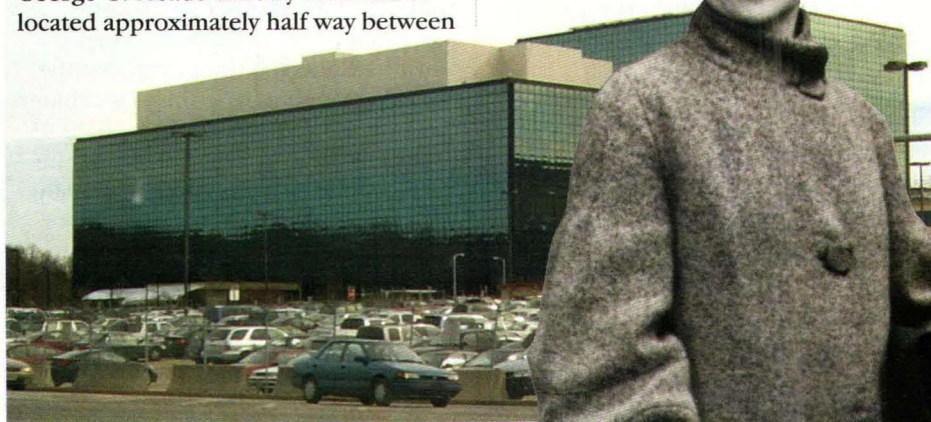


L-R: Patrick Weadon - Curator of the National Cryptologic Museum [NCM], David Hamer - Vice-Chairman of Acquisitions & UK Liaison Officer NCMF, MG John E. Morrison, USAF (Ret.), President of NCMF Eugene J. Becker, Vice-President of NCMF David D'Auria - Chairman of Acquisitions NCMF [NCMF = National Cryptologic Museum Foundation]

their brilliant contributions but thousands of other men and women have quietly served their country altering the course of this nation's history and ensuring a free and safe America. The history of cryptology is their story."

NSA is headquartered on the Fort George G. Meade military reservation located approximately half way between

prised cryptologic artefacts from not only NSA's brief history but also from the many and varied individuals and organisations associated with the history of cryptology.



Washington DC and the port city of Baltimore, Maryland, at the intersection of the Baltimore-Washington Parkway and State Highway 32. The Agency is about a twenty-minute drive from either of these cities on a good day: though the notorious DC traffic problems can interfere seriously with these estimates!

For forty-one years, the Agency maintained an 'in house' collection and exhibit whose purpose was to educate and inspire both new and veteran civilian employees of NSA and their many military colleagues drawn from the intelligence units of various branches of the US services. The collection com-







Herbert O. Yardley 1889-1958

Herbert O. Yardley - American cryptologic pioneer caused a sensation in 1931 with the publication of his memoirs *'The American Black Chamber'*. In this book, Yardley revealed the extent of US cryptanalytic work in the 1920s. Surprisingly, the wording of the espionage laws at that time did not permit prosecution of Yardley

Especially, it includes historical milestones from events that had an impact on American history including, but by no means limited to, the American Civil War, World Wars I and II, Korea, Vietnam and present-day conflicts in the Middle East.



A familiar 'friend' on exhibit at the museum

In 1993 it was decided at the most senior levels within the Agency to transfer the collection to a location that would be accessible, not only to those 'inside the fence' at NSA but to the general public. Thus, the National Cryptologic Museum became, and remains to this day, the only historical collection of a secret government agency or department within the USA that is open to viewing by the public and for study by cryptologic scholars.

Left: Elizebeth Smith Friedman - cryptanalyst, and pioneer in US cryptology. Although she is often referred to as the wife of William Friedman, she enjoyed many successes in cryptology in her own right and has been dubbed "America's first female cryptanalyst"

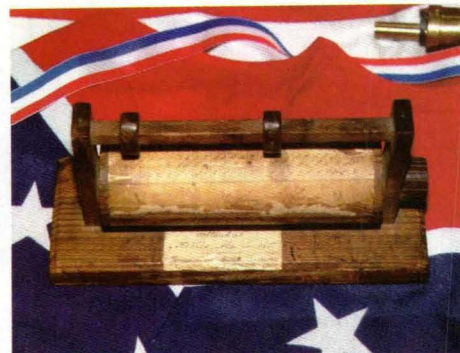
## Union Code Book and Confederate Cipher Cylinder Exhibits

No matter how a message was transmitted, wigwag, telegraph, or written, for security purposes, it was often encoded or enciphered. A code changes a word or phrase into a different word, phrase, or number group; a cipher substitutes



each individual letter for a different letter, number, or symbol. Here are two examples of such systems.

Although entitled Cipher for Telegraphic Correspondence, this book is actually a code book. It was used by Union General Joseph Hooker's code clerk and is one of the few books whose provenance is known. Important names, places, and military



terms have two different code names.

The Confederate cipher cylinder (above) is one of only two surviving cipher cylinders. Using a Vigenere square, plain text letters and their

corresponding cipher letters are indicated by the position of the pointers. Each system has its benefits and disadvantages, but both offered an excellent level of security.



## GRAB II Elint Satellite Exhibit

The GRAB II (Galactic Radiation And Background) satellite model, on loan from the NAVAL Research Lab (NRL,) depicts the second Signals Intelligence satellite to be launched by the United States. The first GRAB satellite launched on 22 June 1960 followed the loss of the U-2 spy plane flown by Gary Powers in May. On 29 June 1961, the GRAB II was successfully launched.

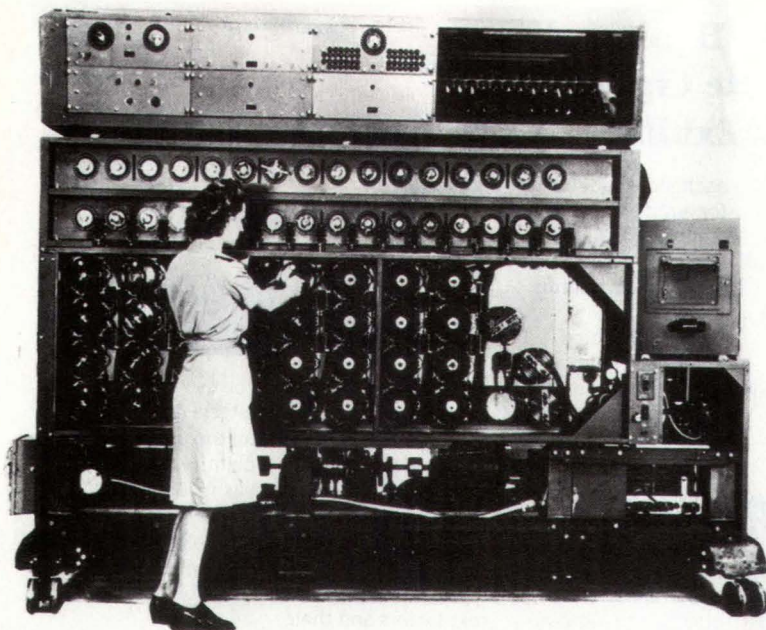
## Cray Supercomputers



Working with companies, such as Cray Research Inc., NSA has been a leader in computer development throughout its history. Some of the earliest supercomputers were designed and built for the National Security Agency.

On exhibit in the museum are two Cray supercomputers. The XMP-24 on display is the upgrade to the original XMP-22 that was the first supercomputer Cray ever delivered to a customer site. It was in operation from 1983 to 1993 and was arguably the most powerful computer in the world when it was delivered. It used serial processing to conduct 420 million operations per second.





## BEATING ENIGMA WITH BOMBES

The British Bombes worked through rotor settings in the opposite direction of the Enigma. Since the Bombe needed to try every combination of rotor settings, it didn't matter from which direction this was accomplished. Even though it represented the slowest moving Enigma rotor, the top Bombe drum spun the fastest at 50.4 rpm. In the instant that each position made contact, an electrical current tried to complete a path through each of the test registers and the diagonal board. Most could not complete the path correctly and were discarded. Those that did complete the path caused the machine to stop.

Members of the Women's Royal Naval Service, Wrens, operated the machines, and when the machine found a "stop" the operator wrote down the rotor settings. She then reactivated the Bombe enabling it to search for any other possible solutions within that wheel order. Another Wren tested the stop on a checking machine and passed the result to a cryptanalyst in another building. When the cryptanalysts found the one correct setting, they notified the Wrens to stop work on that message and move on to the next. It took ten minutes for the Wrens to change the wheel order for the next run and an additional thirty-five to fifty minutes to set up the connections and rotor positions.

## Letter from Fort Meade

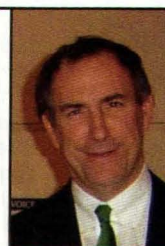
NCM maintains an extensive library for use by visiting researchers and hosts students at all levels from intermediate public school grades to post-graduate.

NCM has been described in official literature as "NSA's principal gateway to the public... it shares the nation's, as well as NSA's, cryptologic legacy and place in world history." Approximately fifty thousand visitors a year pass through the doors of the museum, which began life as a motel. Many of these visitors are having their first "peek into the secret world of codemaking and codebreaking."

Adjacent to NCM and accessible via a brief stroll along a path through a pleasant, wooded area is the National Vigilance Park, a static exhibit containing examples of aircraft, used by US armed forces, that commemorates the lives of those lost during reconnaissance flights.

High points of Fort Meade activity during the past year or so are the departure of the Director of NSA, Lieutenant General Michael V. Hayden, USAF, who has served in that position since 1999: he moves on to the position of Principal Deputy Director of National Intelligence, with the addition of a fourth star. Lieutenant General Keith B. Alexander, USA, succeeds General Hayden as Director. Another outstanding event was the retirement and departure from NCM of the long-time

Curator of the museum, Jack Ingram, who served in that assignment for most of the first twelve years of NCM's existence, having been preceded briefly in the post by the founding-Curator, Jerry Coates. Patrick Weadon (above-right), the new Curator of the museum, assumed his duties in January of 2005 after many years of service in management posts within the Agency, during which time he was very active in the study of the Agency's history. He is the author of numerous publications from NSA's Center for Cryptologic History [CCH].



Patrick Weadon

**LINKS:** [www.nsa.gov/museum](http://www.nsa.gov/museum)

# MAGIC

## SECRET SIGNALS AND THE ART OF DECEPTION

### How disinformation helped the codebreakers

**W**hen cryptanalysts broke several Japanese ciphers prior to the attack on Pearl Harbor, Hawaii, little did they know it would be the start of a major operation that would ultimately provide a turning point in WWII.

Just hours before the naval base was attacked, one intercepted cipher revealed that Japanese diplomats and military officials in Washington had been told to destroy their cipher machines and code books. Though this was later judged to have been a key moment that could have revealed

Japanese intentions, there was nothing to suggest Pearl Harbor (specifically) was about to be bombed. Though warnings were issued to several key military locations, delays in communications meant that these vital transmissions arrived too late. Japan's surprise attack was the prelude to several victories in Malaya, the Dutch East Indies, the Philippines, Burma and other countries.

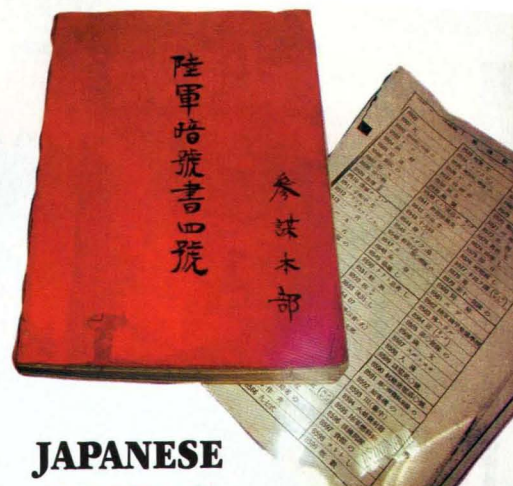
Intercepting Japanese signals traffic was now a priority - at the very least it could provide clues to Tokyo's next



Pearl Harbor under attack

target. Leading the effort, code-named Magic, was the US Navy's Combat Intelligence Unit, called OP-20-G and





## JAPANESE 'ENIGMA'

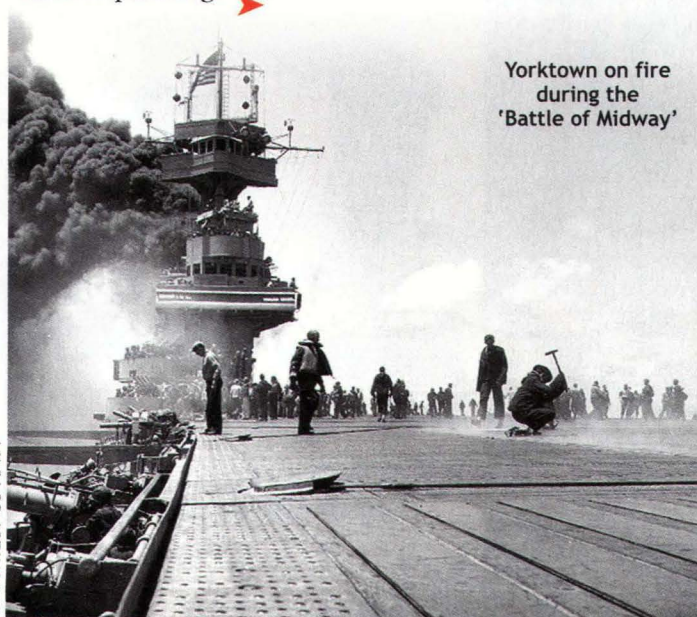
The Germans manufactured Enigma machines for the Japanese Government but they were never received. 'Officially', they were lost when the submarine tasked with the delivery was sunk. Japanese experts, having very basic shared knowledge of the Enigma, created their own device. Only two surviving examples of the Japanese Enigma are known to exist.

consisting of 738 naval personnel. In April 1942, a message in Japan's JN25 (first introduced on 1 June 1939) naval cipher was decoded. The Allies learned that the Solomon Islands and New Guinea were likely targets. US Navy warships set out across the Coral Sea to confront the Japanese. In the end, both sides lost an aircraft carrier but the invasion fleet was thwarted.

Japanese intelligence officials considered the possibility that the US had managed to decode its secret ciphers. However, the crucial question for the Allies was where would the next attack occur? Military planners believed India, Australia or Hawaii were all possible targets. It was essential to obtain accurate data to help formulate defence planning.



Japanese carrier  
Hiryu on fire



Yorktown on fire  
during the  
'Battle of Midway'

COURTESY US NAVY

## CAPTAIN JOSEPH J. ROCHEFORT 1898-1976

Captain Joseph John Rochefort was a major figure in the US Navy's cryptologic and intelligence developments from 1925 to 1947. He headed the Navy's fledgling cryptanalytic organisation in the 1920s and provided singularly superb cryptologic support to the US fleet during World War II, leading to victory in the war in the Pacific. At the end of his career (1942-1946), Rochefort successfully headed the Pacific Strategic Intelligence Group in Washington.



Rochefort was born in 1898 and enlisted in the navy in 1918. He was commissioned an ensign after graduation from the Stevens Institute of Technology. Rochefort's tours ashore included cryptanalytic training under both Captain Laurance Safford and Agnes Meyer Driscoll in 1925; a stint as second chief of the Department of Naval Communications' newly created cryptanalytic organisation, OP-20-G, from 1926 to 1929; training in the Japanese language from 1929 to 1932; and a two-year intelligence assignment in the Eleventh Naval District, San Diego, from 1936 to 1938. Until 1941, Rochefort spent nine years in cryptologic or intelligence-related assignments and fourteen years at sea with the US fleet in positions of increasing responsibility.

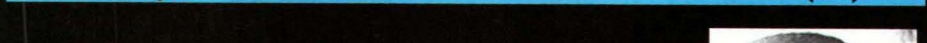
In early 1941, Laurance Safford, again chief of OP-20-G in Washington, sent Rochefort to Hawaii to become Officer in Charge (OIC) of Station Hypo in Pearl Harbor. The reasons for Rochefort's appointment were obvious: he was an expert Japanese linguist, an experienced and very talented intelligence analyst, and a trained cryptanalyst.

Rochefort hand-picked many of Hypo's augmentees, and it contained the Navy's best cryptanalysts, traffic analysts, and linguists, including Thomas Dyer, Wesley A. (Ham) Wright, Joseph Finnegan, General Alva Lasswell, Thomas Huckins, and Jack Williams.

After the Japanese attack on Pearl Harbor, Rochefort and the Station Hypo experts were eventually able to read enough of Japanese naval communications to provide daily intelligence reports and assessments regarding Japanese force disposition and intentions. Station Hypo provided accurate and timely intelligence reports for the rest of the Pacific War; these reports were used by the most senior navy officer for strategic and tactical decisions.

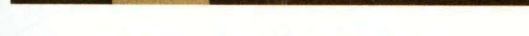
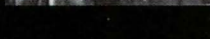
Rochefort died in 1976. In 1986, he posthumously received the President's National Defense Service Medal, the highest military award during peacetime, for his support to the Battle of Midway.





Analysts had decoded messages that indicated two targets, but these were coded simply as AL and AF. Officials believed AL was code for the Aleutian Islands, but that this may have been a diversion for their primary objective - AF. It was therefore of immense impor-

A deception plan was needed. Commander Rochefort (above) knew that Midway's relied heavily on a water filtration plant for its drinking water. On 10 May he ordered a plain text message to be sent from Midway to

[illegible]





JN means simply Japanese Navy, and JN-25, consisting eventually of about 33,000 words, phrases, and letters, was the primary code the Japanese used to send military, as opposed to diplomatic, messages

the Americans unprepared. A major battle ensued. The US lost 307 men, one carrier (the Yorktown,) one destroyer, and 147 aircraft. However, the Japanese losses were far greater and more significant - 2,500 men, four carriers, one heavy cruiser, and 332 aircraft.

The balance of power in the Pacific had shifted - though it would not have been possible without the dogged determination of code breakers, and a simple deception operation.

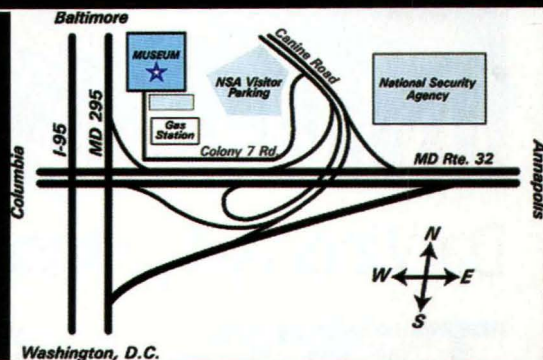


# National Cryptologic Museum



## Free Admission

- Exhibits
- Map and Directions
- Museum Field Trips
- Museum Library
- Gift Shop
- National Vigilance Park



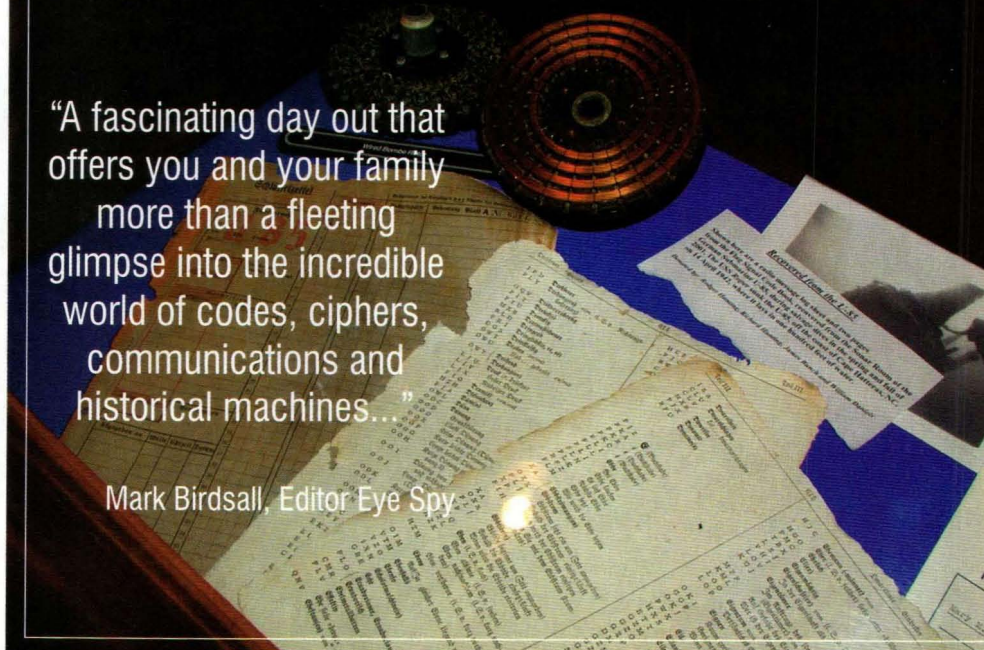
**Open to the Public:**  
**Monday-Friday 9:00-4:00**  
**1st and 3rd Saturdays 10:00-2:00**  
**Closed Sundays and**  
**Federal Holidays**  
**301-688-5849**

**Group tours should be scheduled in advance**

Radio message log and two pages from the Flag Signal Code Book, recovered from the sonar room of the German submarine U-85, during salvage dives in 2001

"A fascinating day out that offers you and your family more than a fleeting glimpse into the incredible world of codes, ciphers, communications and historical machines..."

Mark Birdsall, Editor Eye Spy







## Britain's 'FBI' Appoints Former MI5 Director

**S**tephen Lander, a former MI5 Director, has been appointed as the head of the British Government's newly created Serious Organised Crime Agency (SOCA), dubbed the 'UK's FBI' by intelligence

## Da Vinci Judge Inserts Secret Code in Court Ruling

**T**he judge presiding over a court case involving Dan Brown's best-seller *The Da Vinci Code*, actually embedded a coded message in his judgment. Justice Peter Smith admitted his secret after London solicitors became puzzled by a series of odd italicizations in the judgement. The lawyers thought the wording unusual and embarked upon a mission to see if Smith had indeed created a code of his own.

Justice Peter Smith told reporters his action was just a bit of fun. He secreted a reference to the inventor of the Royal Navy's first modern warship into his ruling using the "Fibonacci Sequence." This simple code is

a combination of a mathematical progression and letter substitutions also used by Dan Brown in his book. Solicitor Dan Tench, who works at the law firm Olswang, is claiming "first code-breaking rights" - the message reads: "Jackie Fisher who are you Dreadnought."

Fisher, a 19th-century admiral, is generally credited with developing 'Dreadnought', a battleship equipped with six or more guns. "The message reveals a significant but now overlooked event that occurred virtually 100 years to the day of the start of the trial," Justice Smith said today in a statement. "The preparation of the code took about 40 minutes and its insertion another 40 minutes or so. I hate crosswords and do not

do Sudoku as I do not have the patience."

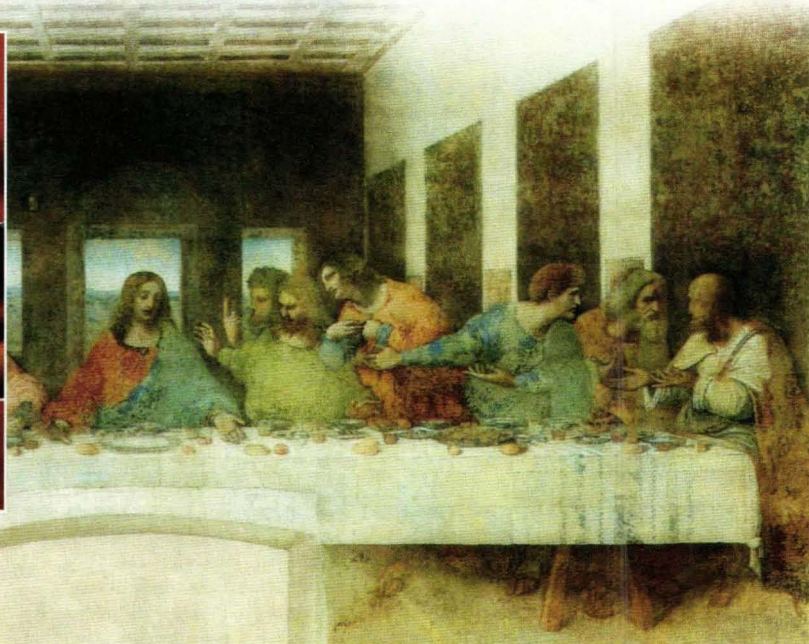
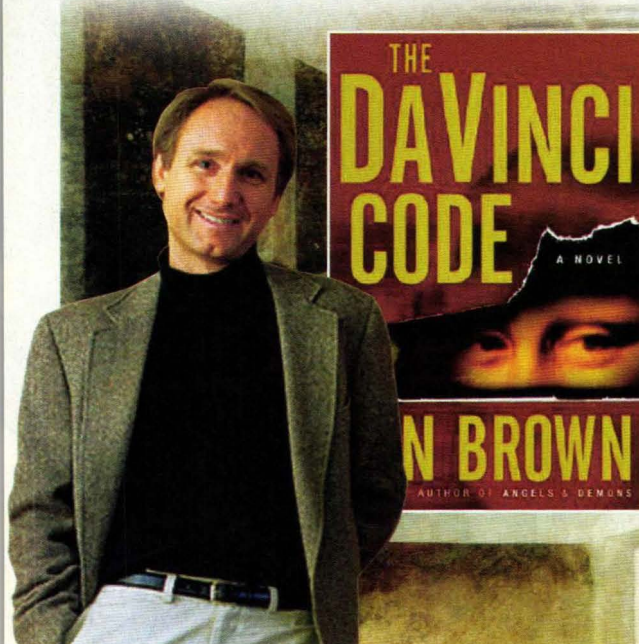
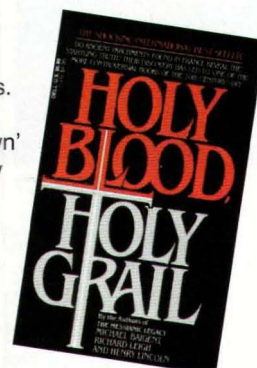
Dan Brown was cleared of "plagiarizing the plot" of *The Da Vinci Code* from Richard Leigh and Michael Baigent, co-writers and researchers of the equally controversial *Holy Blood, Holy Grail*. Both men accused Brown of making millions off their theories that Jesus Christ married Mary Magdalene and fathered a child, spawning a royal dynasty. Brown, of course, writes that the blood-line still exists.

While *The Da Vinci Code* is generally acknowledged as a brilliant, though controversial piece of fiction, Leigh and Baigent's work is described as non-fiction and has been

extensively used by researchers. Not that Dan's Brown's book is any less researched or thought out.

*The Da Vinci Code* has sold 40 million copies worldwide - far more than *Holy Blood, Holy Grail*. However, since its appearance, sales of Leigh and Baigent's book have also spiralled.

Justice Smith says he was just having a "bit of fun." Indeed, the judge's 71-page decision began by spelling out "Smithy code."





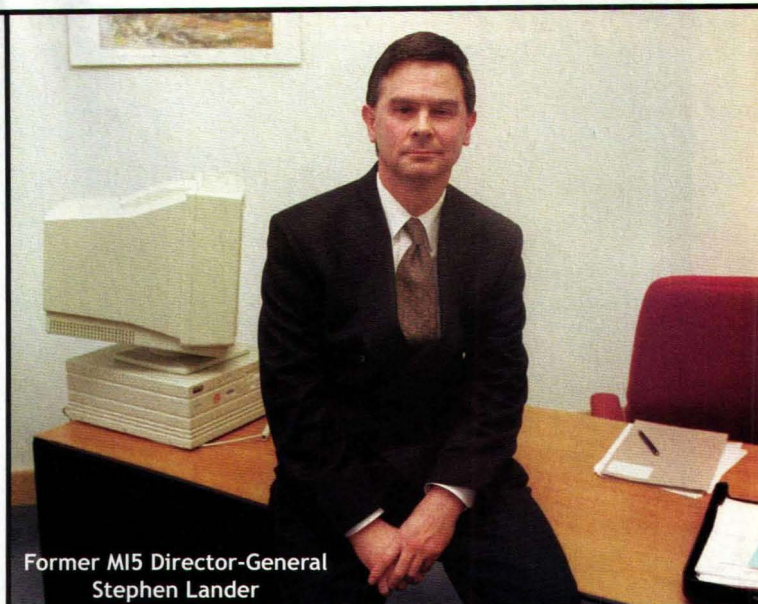
watchers. The agency will have widespread powers of search, seizure, arrest and interrogation.

Many of its officers will be based at secret locations throughout the country. They will have the combined powers of police, immigration and customs officers and will be able to conduct widespread surveillance and intelligence-gathering.

SOCA will mount operations against overseas targets and be able to strike 'Queen's Evidence' deals with informants. This is regarded as a most powerful

weapon and should enable the agency to make written agreements with suspects who are willing to testify against leading figures in the underworld. The 'deals' will be made known to judges and juries. When fully operational, SOCA will have a staff of more than 4,000 officers, many including electronic, surveillance and firearms experts. Some 50 SOCA units will be spread across the country.

Eye Spy understands its secret headquarters are based in Whitehall, London.



Former MI5 Director-General Stephen Lander

## RED MERCURY UK TERRORISM 'PLOT'

**T**he trial of three men, accused of conspiring to purchase Red Mercury - a supposedly highly dangerous material, has started at the Old Bailey Court in London.

According to the prosecution, the suspects planned to sell hundreds of pounds of Red Mercury to a Middle East terrorist via an intermediary. Unbeknown to the men, the 'middle man' was none other than Mazher Mahmood, an undercover reporter for the UK's most popular Sunday newspaper - *The News of the World*. He told the men that Red Mercury sold at £300,000 (\$500,000) a kilo.

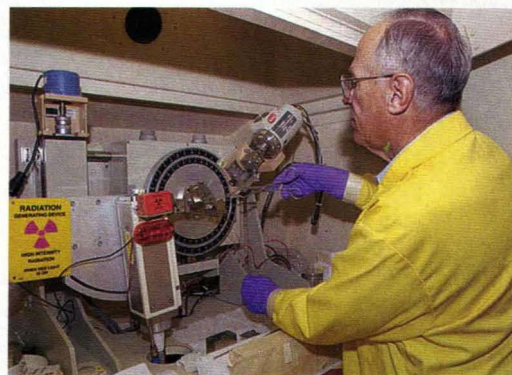
The court heard that Mahmood had secretly recorded conversations with the suspects - Roque Fernandes, 44, Abdurahman Kanyare, 53, and Dominic Martins, 45, in the

Autumn of 2004. After gathering as much information as possible, the journalist handed Scotland Yard his file and the men were subsequently arrested.

Prosecutor David Ellison acknowledged that the suspects "motive" was probably financial reward, but the consequence of Red Mercury finding its way to terrorists was alarming. "The circumstances of the deal they were pursuing was such that each of them knew the intended customer may well have wanted the substance for use in terrorism," Ellison said. "The tape-recorded evidence shows clearly that each of these defendants did agree to pursue the purchase of this radioactive substance at a price of hundreds of thousands

of pounds, knowing it was the sort of thing used in acts of terrorism."

The newspaper had learned of the plot through a banker, referred to in court as 'Mr B'. He had been contacted by Martins who said he wanted to buy the radioactive material.



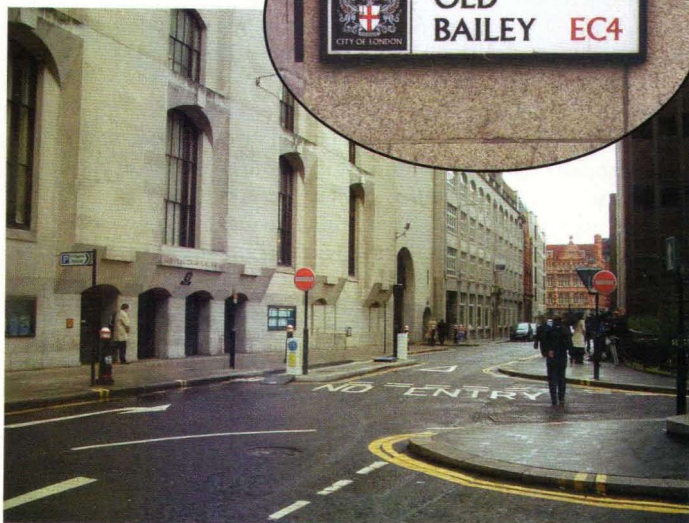
Mahmood, who was acting undercover on behalf of the anti-terrorism branch as an authorised informant (covert source), is a controversial figure and is famous for a well known sting operation when he impersonated a "fake sheikh." The prosecution say the defence may accuse him of "blatant entrapment" but say vital intelligence was also gathered by the police in interviews with the suspects. "The prosecution acknowledge there is controversy surrounding some of his work. I want to underline a fundamental feature of the core evidence the prosecution rely on. The core evidence is what the defendants themselves have said, pre-arrest in tape-recorded meetings or after arrest in police interviews."

All three suspects deny "entering into a funding arrangement for the purposes of terrorism and one of conspiracy to possess an article for terrorist purposes."

### RED MERCURY - DOES IT EVEN EXIST?

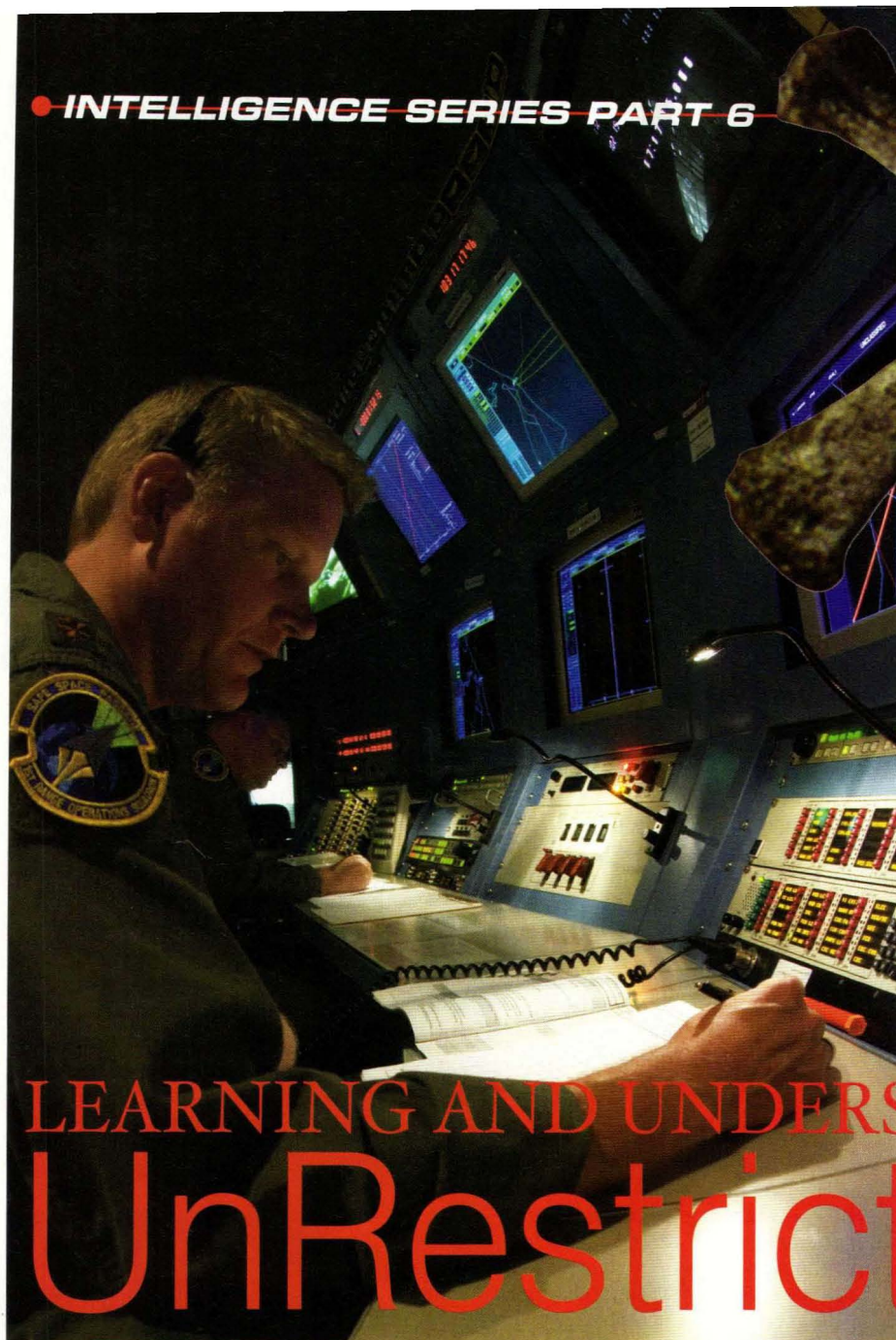
Controversy about 'Red Mercury' exists - even in the scientific community. Some experts say the material is "mythical," but others disagree, including Sam Cohen, creator of the neutron bomb. He believes sufficient evidence exists to show that the Soviets produced "vast quantities" of mercury antimony oxide, the intermediate - and equally elusive - compound from which red mercury is supposedly produced by placing it inside a nuclear reactor. "There's no doubt that they made a large amount of that stuff. I've talked to chemists who have analysed it in East Germany," he says. "But what they did with it is a mystery."

An official at The International Atomic Energy Authority (IAEA) in Vienna supposedly told reporters. "Red mercury doesn't exist."



MAIN PICTURE: © KEVIN FULTON. INSET: STEVE MCMANUS/LEPL





following a legal declaration of war, as defined by international law

**a) Land:** Where fighting is based on foot soldiers and land resources such as tanks, artillery and other ground vehicles

**1. Guerilla warfare:** Unconventional tactics for advantage in a conflict  
**b) Sea:** Fighting



# LEARNING AND UNDERSTANDING INT UnRestricted Warfare

**U**nRestricted Warfare is a relatively new concept first defined in 1999 by two Chinese colonels in a book written in the late 1990s for the Chinese People's Liberation Army. The authors, colonels Qiao Liang and Wang Xiangsui describe un-conventional tactics that could be used by an enemy against more powerful targets. This concept has continued to evolve and now consists of fifteen different modalities of warfare employed against an enemy and poses a unique threat to leading world powers that have increasingly been targeted with small scale, stealth-focused attacks on non-military targets. The book points out that leading powers have not considered the wider picture of military strategy, which includes legal and economic factors as a method of warfare. Since no consideration has been given to these aspects of conflict, major powers are highly vulnerable to attacks along these lines.

## FULL SPECTRUM OF WARFARE MODALITIES

Warfare is defined as organised conflict between groups for political, economic, or religious purposes. Each group is motivated by a common purpose. We can categorise it using modalities or types of warfare. Traditionally we have only considered two types - Conventional and Weapons of Mass Destruction. However with the technological advancements that have been occurring in the world, 15 new areas, or modalities of warfare are recognised. These are now known as the modalities of UnRestricted Warfare. Here is a brief description of each of these modalities.

### Traditionally Recognised Modes of Warfare

**1. Conventional Warfare:** Fighting between armed forces from nations

based on ocean going assets such as aircraft carriers, destroyers and other vessels

**1. Under-sea warfare:** The use of submarines to attack ocean going vessels of an adversary in a conflict

**c) Air:** Where fighting is based on planes, missiles and air based assets

**2. Weapons of Mass Destruction (WMD):** Nuclear, chemical or biological, that kills or injures large numbers of civilians as well as military personnel

**a) Chemical:** Chemical weapons associated with military operations that use toxic properties of chemical substances to kill, injure or incapacitate an enemy

**b) Biological:** The use of any organism such as bacteria, viruses or other disease-causing organism or toxins found in nature, as a weapon of war

**c) Nuclear:** A weapon that derives its energy from nuclear reactions of fission and/or fusion





In this training brief, Eye Spy associate editor Kevin Coleman examines the emerging threat of UNRESTRICTED WARFARE and identifies several new and important areas that individually or combined pose a major threat to world governments. The implications for the intelligence world are significant...

## UNRESTRICTED WARFARE MODALITIES

The following modalities represent additional types of warfare that make up the category of unrestricted warfare.

**3. Cultural warfare:** Actions and tactics designed to bring about change that target human activities, knowledge, customs, and arts of a group of people.

**4. Economic warfare:** Actions and tactics designed to bring about change that target the organisation of production and distribution of goods and services within a state governed

**8. International law warfare:** Actions and tactics designed to undermine the regulations and/or policies of international or multinational organisations or to provide an adversarial nation with a major strategic advantage over another.

**9. Information and media warfare:** Actions and tactics designed to influence the opinion of people and foreign news media by manipulating information distributed openly.

**10. Telecommunication & network warfare:** Actions and tactics designed to disrupt electronic transactions or communication of a targeted adversary.

**11. Political warfare:** Actions and tactics designed to bring about regime or policy change within an adversarial nation state.

**12. Psychological warfare:** Actions and tactics designed to target the morale, mental or emotional component of an adversary.

**13. Resource warfare:** Actions and tactics designed to inhibit access to critical supplies or natural resources needed by an organisation, group or nation.

**14. Smuggling warfare:** Actions and tactics designed to flood an adversary's markets with illegal, counterfeit goods or products in an effort to create economic loss.

**15. Technological warfare:** Actions and tactics designed to capture intellectual property associated with civilian or military technology that creates economic or technical advantage.

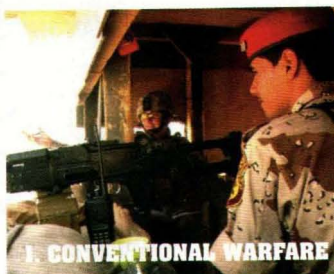
system - increase and decrease in economic aid is a tactic of economic warfare.

**5. Environmental warfare:** Actions and tactics designed to intentionally spoil the natural environment or modify the ecological or earth systems of your adversary.

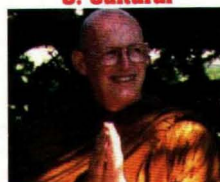
**6. Financial warfare:** Actions and tactics designed to undermine or create a loss in confidence in the monetary or financial systems including currency, banks and the stock market of an adversarial state.

**7. Illegal drugs warfare:** Actions and tactics designed to flood an adversarial state with addictive illegal controlled substances.

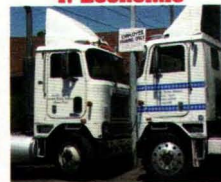
## UNRESTRICTED WARFARE Full Spectrum of Warfare Modalities



3. Cultural



4. Economic



5. Environmental



6. Financial



7. Illegal drugs



8. International law



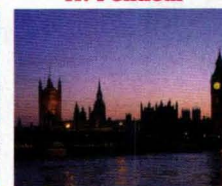
9. Information/Media



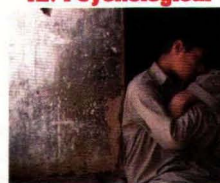
10. Telecommunications



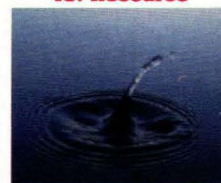
11. Political



12. Psychological



13. Resource



14. Smuggling



15. Technological



16. Terrorism



17. Gangs



**16. Terrorist warfare:** Refers to the unlawful actions and tactics designed to intimidate governments or societies, often to achieve political, religious, or ideological objectives. For example:

- a. Small Arms: Weapons carried into battle by individual infantry soldiers, including pistols, rifles and machine guns.
- b. Car Bombs: A bomb that is placed in a car or truck and is intended to be exploded while inside the vehicle.
- c. Improvised Explosive Devices: A formal name for

explosive devices as used in unconventional warfare by terrorists, guerrillas or commando forces.

d. Suicide Bombers: Bomb attack on people or property, committed by a person who knows the explosion will cause his or her own death.

**17. Gang Warfare:** Actions and tactics of using a group of individuals who share a common identity (gang) to conduct acts of violence or intimidation.





# HIGH LEVEL ATTRIBUTES COMPARISON

Table One

| URW                         | TRADITIONAL           |
|-----------------------------|-----------------------|
| CHALLENGES INFLUENCE        | CHALLENGES POWER      |
| SURPRISE ATTACKS            | DECLARATION OF WAR    |
| ILL-DEFINED FIELD OF BATTLE | DEFINED BATTLE FIELD  |
| OBSCURER TARGETS            | DEFINABLE TARGETS     |
| COVERT INFILTRATION         | UNIFORMED TROOPS      |
| MULTI-MODAL BATTLEFRONTS    | MILITARY BATTLEFRONTS |
| HIGHLY DYNAMIC              | LOW DYNAMICS          |

Table Two

| Modality                               | Influence Operations |         |           | Current Capabilities |         |           | Primary Weapons                                                                                              |
|----------------------------------------|----------------------|---------|-----------|----------------------|---------|-----------|--------------------------------------------------------------------------------------------------------------|
|                                        | Detection            | Defense | Offensive | Detection            | Defense | Offensive |                                                                                                              |
| 1. Cultural warfare                    | 5                    | 2       | 2         | 2                    |         |           | Open Source Intelligence, internet and information technology                                                |
| 2. Economic Aid warfare                | 4                    | 2       | 3         | 3                    |         |           | Open Source Intelligence, internet and information technology                                                |
| 3. Environmental warfare               | 4                    | 2       | 3         | 3                    |         |           | Open Source Intelligence, internet and information technology                                                |
| 4. Financial warfare                   | 4                    | 2       | 2         | 3                    |         |           | Financial community intelligence, internet and information technology                                        |
| 5. Illegal Drugs warfare               | 4                    | 3       | 4         | 4                    |         |           | Sensory devices, social network analysis, anti-money laundering, HIPAA changes                               |
| 6. International law                   | 4                    | 2       | 3         | 3                    |         |           | Open Source Intelligence, internet and information technology                                                |
| 7. Information & Media warfare         | 5                    | 2       | 3         | 3                    |         |           | Open Source Intelligence, internet and information technology                                                |
| 8. Telecommunication & Network warfare | 4                    | 3       | 3         | 5                    |         |           | Internet, social network analysis, attack tracking and information technology                                |
| 9. Political warfare                   | 5                    | 2       | 3         | 3                    |         |           | Open Source Intelligence, internet and information technology                                                |
| 10. Psychological warfare              | 5                    | 2       | 3         | 3                    |         |           | Open Source Intelligence, social network analysis, cognitive sciences, internet and information technology   |
| 11. Resource warfare                   | 3                    | 2       | 3         | 3                    |         |           | Alternative energy sources, commodity community intelligence, and information technology                     |
| 12. Smuggling warfare                  | 3                    | 3       | 2         | 3                    |         |           | Inspection Technology, social network analysis, authentication technology Open Source Intelligence, internet |
| 13. Technological warfare              | 5                    | 2       | 3         | 3                    |         |           | Open Source Intelligence, social network analysis, internet and information technology                       |
| 14. Terroristic warfare                | 3                    | 4       | 4         | 4                    |         |           | Open Source Intelligence, social network analysis, internet and information technology                       |
| 15. Gang Warfare                       | 3                    | 3       | 3         | 3                    |         |           | Open Source Intelligence, social network analysis, internet and information technology                       |

1 = low 2 = moderate 3 = average 4 = substantial 5 = significant

Awareness of this multi-modal threat is growing. Much more attention is being given to *threat analysis* and the subsequent development of new strategies and technologies needed to address each of these threats. The nature of the URW threat mandates new tactics, approaches, and a new mindset in the effort to combat this threat. Governments must adopt a new National Defense and Security Strategy that is designed based on the unique attributes of URW. When we look at conflict we tend to look at land, sea and air combat. URW is different. The physical aspects of conflict are obscured. At a high level, the table (see Table One right) contrasts URW Warfare with Conventional Warfare.



Current threats represent a new way of thinking about conflict and warfare. What it takes to successfully defend against and offensively leverage this new era of Unrestricted Warfare is radically different from that which determined success in asymmetric warfare in the past. The battlefield now includes the intellects of people and cyberspace. It is a battle for the minds of individuals, as well as for influence over culture, values and beliefs. Multiple aspects of life are attacked in an effort to influence and bring about change rather than focusing on attacking life itself. These tactics include disruption of everyday life and destruction of cultural symbols that are core to the opponent's way of life.

It is important to note that traditional forms of warfare will not disappear anytime soon. More likely, any conflict will include traditional and URW techniques. In this context, nuclear, chemical, and biological weapons fall under the definition of traditional warfare.

Let us look at each of these fifteen areas of URW and assess the risk, potential impact, current defense capabilities, and magnitude of change required to address the threat. The following high-level threat matrix (Table Two) was created using Trans-disciplinary

Intelligence Engineering (TIE) techniques that were used in previous US Department of Homeland Security scenarios development risk analyses. A numeric value between 1 (low) and 5 (significant) has been assigned to each evaluation aspect within the matrix. It is important to keep in mind that this is based on the estimated capabilities, motivation, and resources of our adversaries in each of the fifteen facets of URW. This is based on open source intelligence and does not reflect any classified intelligence.

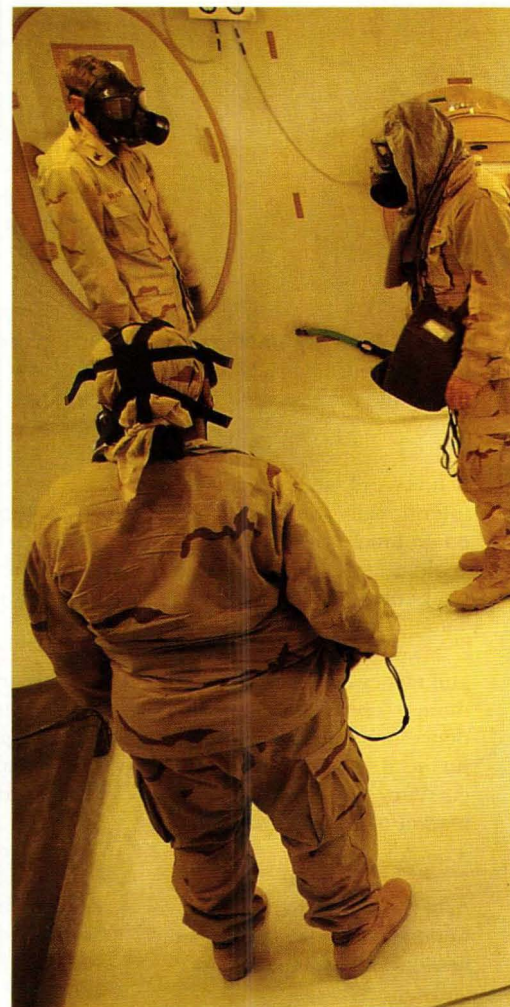
For the most part, anyone of these types of warfare can be planned and launched from anywhere in the world. A small, isolated group with only moderate training and financing can create a significant impact by launching an attack using one or more URW modalities. Creating the capacity to address these threats is arguably the world's biggest challenge. Equally as challenging is creating the weaponry for the "digital warrior" needed to combat these threats as well as an early warning system to detect when one or more of the stealthy URW attacks are launched. Or, once detected, is it too late already?

## MULTI-MODAL ATTACK EXAMPLES

We are currently being engaged by multi-modal attacks across the full spectrum of warfare. This section will examine five modalities of attack and provide evidence that substantiates the claim that we are in an active engagement within each modality. Using the Trans-disciplinary Intelligence Engineering (TIE), OCINT (a forecasting method used by the government as well as other organisations), and URW constructs discussed here, the following data is derived.

## FINANCIAL WARFARE

Example: Attack from North Korea. The North Korean Government is supporting operations that are counterfeiting currency.





Counterfeiting can cause loss of confidence in a monetary system and a devaluation of the dollar as well as moderate economic impact.



#### REAL OR COUNTERFEIT?

**News Article:** *US accuses North Korea of conspiracy to counterfeit.*  
 "Irish rebels, a major Asian bank and Chinese gangsters also implicated in a government-backed scheme to flood American economy with phony \$100 bills." Josh Meyer, Barbara Demick, *Los Angeles Times*. 18 December 2005  
 LINK <http://www.sfgate.com/cgi-bin/>



article.cgi?f=/c/a/2005/12/18/MNGLVG863T1.DTL&feed=rss.news

#### Telecommunications & Network Warfare Example: *Under Attack from Global Sources*

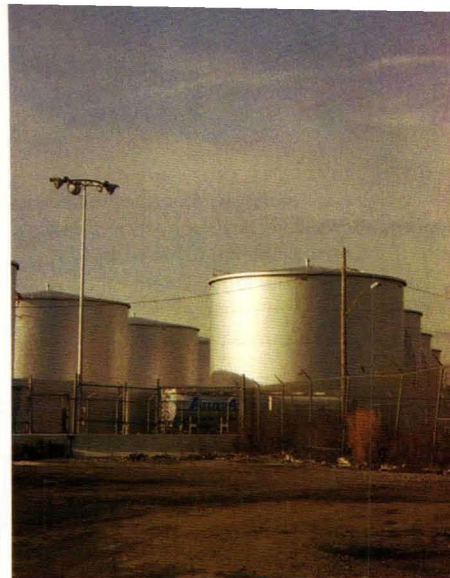
"Based on last month statistics, in the last minute there has been over 50,000 serious computer attacks reported. In addition, there is an average of 250 viruses released monthly. Additionally, incidents of attack increased nearly six times since 2000 according to industry metric."



**News Article:** "2006 was barely under way when a recently discovered flaw in Microsoft Windows prompted Symantec Security Response to raise its ThreatCon rating to Level 3 (or 'high') for the first time since July of 2004." 6 March 2006  
 LINK <http://www.ameinfo.com/79557.html>

#### Resource Warfare Example: *Threat of an attack by President Hugo Chavez*

"Venezuela's President Hugo Chavez has warned he was taking potential steps to cut off oil shipments to the United States

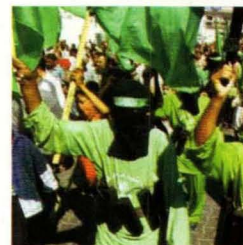


in the event Washington goes too far campaigning against his elected rule."

**News Article:** "Iran and al-Qaida threaten oil embargo and economic warfare." 18 February 2006 LINK <http://www.asianews.itview.php?l=en&art=5564>

**Political Warfare Example: *Offensive move against HAMAS Government***  
 "US and Israel meet secretly to explore ways to remove HAMAS"

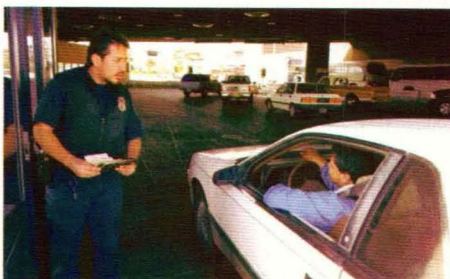
**News Article:** "Hamis protested 'interference' by the United States and Israel following reports the nations were exploring ways to topple the militants incoming government unless they renounced their violent ideology and recognised Israel's right to exist."



14 February 2006 LINK <http://www.msnbc.msn.com/id/11339817/>

**Illegal Drug Warfare & Terroristic Warfare Gang Warfare Example: *Threat of attack from multiple sources***  
 "Drug smugglers threatening [to] use MS-13 gangs to kill Border Patrol."

**News Article:** "Homeland Security Department alerted that gangs are planning coordinated attacks along the US-Mexico border and smuggling weapons to Iraqi nationals in the USA." 31 January 2006 LINK <http://www.msnbc.msn.com/id/11116179/>





# Table Three

| Modality                               | Influence Operations | Current Capabilities |         |           | Primary Weapons                                                                                               |
|----------------------------------------|----------------------|----------------------|---------|-----------|---------------------------------------------------------------------------------------------------------------|
|                                        |                      | Detection            | Defense | Offensive |                                                                                                               |
| 1. Cultural warfare                    | 5                    | 2                    | 2       | 2         | Open Source Intelligence, internet and information technology                                                 |
| 2. Economic Aid warfare                | 4                    | 2                    | 3       | 3         | Open Source Intelligence, internet and information technology                                                 |
| 3. Environmental warfare               | 4                    | 2                    | 3       | 3         | Open Source Intelligence, internet and information technology                                                 |
| 4. Financial warfare                   | 4                    | 2                    | 2       | 3         | Financial community intelligence, internet and information technology                                         |
| 5. Illegal Drugs warfare               | 4                    | 3                    | 4       | 4         | Sensory devices, social network analysis, anti-money laundering, HPAAs changes                                |
| 6. Information law                     | 4                    | 2                    | 3       | 3         | Open Source Intelligence, internet and information technology                                                 |
| 7. Information & Media warfare         | 5                    | 2                    | 3       | 3         | Open Source Intelligence, internet and information technology                                                 |
| 8. Telecommunication & Network warfare | 4                    | 3                    | 3       | 5         | Internet social network analysis, attack tracking and information technology                                  |
| 9. Political warfare                   | 5                    | 2                    | 3       | 3         | Open Source Intelligence, internet and information technology                                                 |
| 10. Psychological warfare              | 6                    | 2                    | 3       | 3         | Open Source Intelligence, social network analysis, cognitive sciences, internet and information technology    |
| 11. Resource warfare                   | 3                    | 2                    | 3       | 3         | Alternative energy sources, commodity community intelligence, and information technology                      |
| 12. Struggling warfare                 | 3                    | 3                    | 2       | 3         | Inspection Technology, social network analysis, authentication technology, Open Source Intelligence, Internet |
| 13. Technological warfare              | 5                    | 2                    | 3       | 3         | Open Source Intelligence, social network analysis, internet and information technology                        |
| 14. Terroristic warfare                | 3                    | 4                    | 4       | 4         | Open Source Intelligence, social network analysis, internet and information technology                        |
| 15. Gang Warfare                       | 3                    | 3                    | 3       | 3         | Open Source Intelligence, social network analysis, internet and information technology                        |

1=low 2=moderate 3=average 4=substantial 5=significant

While these are single source references and reports, there are other supporting pieces of data that are available and that would be linked to the fundamental threat detection and warning systems that are needed to address the multi-modal threat of URW.

In the Cold War NATO used satellite imagery to monitor areas and alert us to troop or military asset redeployment or even a launch of a rocket. The fifteen URW modalities represent tactics used to influence the perception and behaviour of the global population.

A recent example of how such influences can have wide reaching implications are the controversial cartoons published by a Danish newspaper that depicted the Prophet Mohammed. The cartoons caused an angry reactions from Muslims. Some people were incited by religious clerics and anti-Western government agencies, but the media played a significant role and has emerged as a powerful weapon. There are many examples of how information in the media can and is used to invoke response or influence opinion. This is just one example of URW being employed against an adversarial nation.

At the present time we do not possess the early warning detection capabilities needed to address all 15 modalities. Table 3 rates each modality along the following: factors that influence operations, our ability to detect, defend and attack for each modality and finally core technologies that can be used to create an early warning capability.

Given this information, what is clearly required is a global intelligence system that monitors early warning signs for each of the fifteen modalities of URW. Information



A corporate executive is led away after pleading guilty to charges related to accounting fraud. In 2002, the rate of USA corporate criminal probes has gone up, and a record 598 civil enforcement actions were brought against individuals and companies accused of breaking securities laws - another example of UnRestricted Warfare?

superiority is an integral part of offensive and defensive superiority. As illustrated in Table 3, currently we have a limited ability to detect the URW modalities of attack and have only a minimal ability to defend or counter-attack.

The next step in understanding URW is to evolve the concept of a multi-modal early

warning and detection capability that is focused on information warfare directed at a nation. The early warning system would model multiple modalities using Scenario-based Intelligence Analysis (SBIA). By leveraging the insightful aspects of modelling each modality, the output will create case examples of attacks in order to fully understand the

methods and techniques of attack for a given modality or set of modalities. This foundation can be used to create an information-based capability currently needed to defend against any of the fifteen modalities of URW. A derivative benefit from this work will be offensive weapons for all fifteen modalities. The insight and foresight created by this attack modelling and simulation will accelerate the efforts to create a digital weapons cache for military operations.

It is important to note that several of these concepts were vetted at the 2006 Intelligence Summit in front of an international audience from the intelligence, defense and security community resulting in a very positive review.

**SUMMARY:** The concept of URW brings to light alternative methods of attack that can be launched by a small group of individuals on anyone from anywhere in the world against a stronger and more powerful nation. There are no declarations of war; no uniforms; just inflicted damage on an adversary. The blind, sucker-punch attacks are not designed to control areas but rather to influence public opinion, political policies and the opinions of the mass population. When contemplating URW, it is important not to fall victim to singularity. It is uncommon for only one modality to be used in an assault or an attack. Multi-modal attacks will become the modus operandi of URW warriors.

## Intel Examination

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 UnRestricted Warfare 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) can also be downloaded at [www.eyespyimg.com](http://www.eyespyimg.com)

For additional training briefs visit: [www.spy-ops.com](http://www.spy-ops.com)



## TEST YOUR SKILLS



# SLEEPER CELLS

Continued from page 41

made with companies throughout the state. One company reported the theft of about one ton of ammonium nitrate fertiliser from its factory. A police report said an eye witness noted a white van leaving the premises hours after the site had closed. An officer told the detectives sacks of the substance had been stolen.

A search for the van ensued, and within days it was found abandoned and empty on a derelict building site. Detectives now believed that the hire vehicle had been used to transport the sacks from the van. The seeds of suspicion had been sown but was there a terrorist connection? Intelligence officers placed surveillance teams in and around the government building. They were taking no chances. Security was also tightened at other sites.

The only vehicles allowed to stop next to the building belonged to the emergency services. Delivery drivers and staff used a side road - passing through two check points before gaining access. Lessons had been learned following the terrorist attack in Oklahoma City in 1995. Timothy McVeigh parked his lorry packed with explosives directly opposite the FBI building. Ammonium nitrate soaked in nitromethane fuel and supplemented by commercial Tovex explosive was used in the attack. One hundred and sixty eight people lost their lives. The bomb which ripped through a Bali nightclub in October 2002, was also predominately made from fertiliser.

A phone call was then received from the sales manager at a New Jersey firm selling decommissioned emergency vehicles. He explained a caller had enquired how he could obtain an

ambulance for a film set. The manager said they had several vehicles in storage. Two days later a man appeared explaining his previous phone call. Surprisingly he paid in cash and drove the ambulance away. And though most of the insignia had been removed from the vehicle, the livery and interior was still intact. He left no forwarding address or telephone number. The manager was delighted at the sale, but was suspicious and phoned the police. He was surprised the customer did not use a business account or credit card, after all, it was for use in a movie production. After police showed the manager descriptions of the two suspects, he immediately identified one.

Finding the van was a major breakthrough - but could it lead to the two suspects?







# SLEEPER CELLS

Police were asked to monitor the state for a vehicle resembling an ambulance. It was likely the licence plate tags had been replaced and service insignia could have been added.

One mile away from the suspected target building, a local underground station manager had been asked by a CCTV operator to check two men loitering on the platform and making notes. On two occasions the men were seen to catch a train and then return on the opposite platform. They then examined their watch and made notes. He

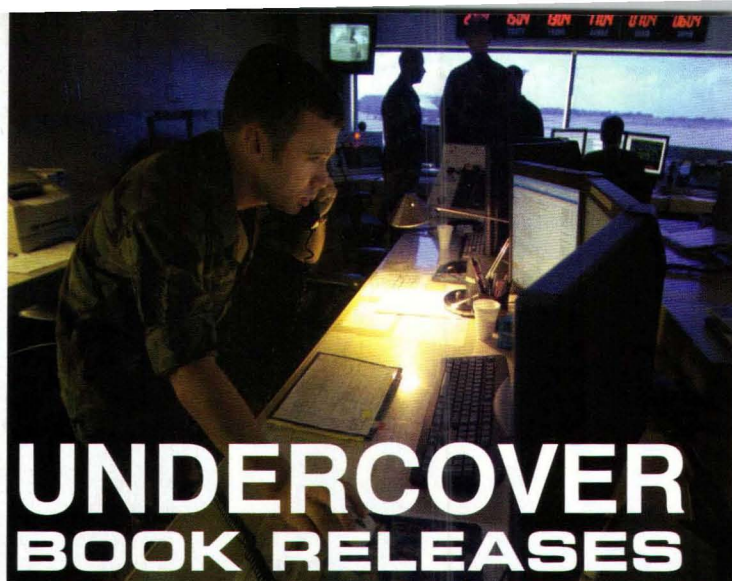
too became suspicious and reported the incident to the police. Detectives examined the CCTV footage, and though not spectacular, they agreed the men were their suspects. Was this their escape route?

It had become a matter of urgency the men were at least questioned about their activity. However, with over eight million people in the state, it was felt unlikely a 'chance meeting' would result in their arrest. Detectives then worked on the theory that the bomb had already been manufactured and placed in the bogus ambulance. If they found its location, then this would probably lead them straight to the suspects. However, it was always possible they could now have departed the scene and another 'team' could have been brought in to 'deliver' the bomb.

Some thirty miles away outside the city, a motel owner demanded to know why two men had seemingly slept in the room of two long-term guests. To her surprise they were same men, but had dramatically changed their appearance and clothes. Both appeared to be wearing uniforms. They offered no explanation, but she called the local police who found the men waiting at a railway stop. They could offer no explanation and were brought in for questioning. The report found its way to the counter-terrorism team who asked that the men be detained.

Within hours the ambulance laden with explosives had been located at a city scrap yard - tucked away amongst other vehicles. A major attack had been thwarted by piecing together often innocuous information.

*Editor's note: At present, few countries have restrictions on the sale of ammonium nitrate fertiliser. It is regarded as one of the easiest materials to obtain and use in a home-made bomb. Eye Spy understands efforts are underway to licence and/or restrict the sale of this innocent substance.*

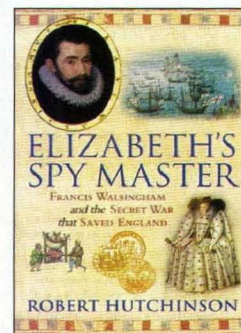


## UNDERCOVER BOOK RELEASES

All prices include postage and packing

**ELIZABETH'S SPY MASTER**  
and the Secret War that Saved England  
Robert Hutchinson  
Orion Books

Francis Walsingham was the first 'spymaster' in the modern sense. His methods anticipated those of MI5 and MI6 and even those of the KGB. He maintained a network of spies across Europe, including double-agents at the highest level in Rome and Spain - the sworn enemies of Queen Elizabeth and her Protestant regime. His entrapment of Mary Queen of Scots is a classic intelligence operation that resulted in her execution.



As Robert Hutchinson reveals, his cypher experts, ability to intercept other peoples' secret messages and his brilliant forged letters made him a fearsome champion of the young Elizabeth. Yet even this machiavellian schemer eventually fell foul of Elizabeth as her confidence grew (and judgement faded). The rise and fall of Sir Francis Walsingham is a Tudor epic, vividly narrated by a historian with unique access to the surviving documentary evidence. Hardback 394pp

Available from Eye Spy Ref: ES/1146 £22.99 \$45.00

**SOE SECRET OPERATIONS MANUAL** Tradecraft Paladin Press

This rare document is the original used to train special agents dropped behind enemy lines in Nazi-occupied Europe during World War II. Used by the British Special Operations Executive (SOE) and its American counterpart, the Office of Strategic Services (OSS), it is an authentic, word-for-word reproduction obtained from a former operative with the clandestine services. It includes sections on ciphers, propaganda, selection of targets, methods of attack, passive resistance, the liaison agent, interrogation and more.

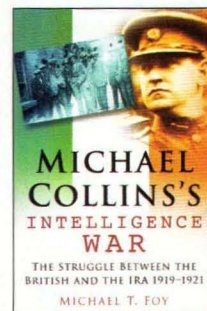


The forerunner of all US Government guides to sabotage, propaganda, interrogation, burglary and other dirty tricks, this extraordinary historical document makes for riveting reading. Softcover. 272pp

Available from Eye Spy Ref: ES/1150 £25.00 \$25.00

**MICHAEL COLLINS'S INTELLIGENCE WAR**  
The Struggle between the British and the IRA 1919-1921  
Michael T Foy  
Sutton Publishing

Michael Collins is often thought of as Ireland's lost leader: a man born into a revolutionary environment who became a skilled statesman and military leader and who met an untimely, violent death. Michael Foy's excellent and thoroughly researched new book looks in depth at Collins's key role in the Anglo-Irish War of 1919-20, and explores the role and personality of this fascinating man. An historical gem. Hardback 281pp



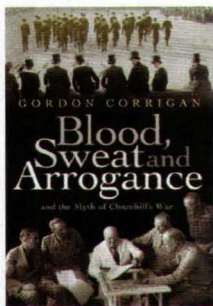
Available from Eye Spy Ref: ES/1152 £22.99 \$45.00



**BLOOD SWEAT & ARROGANCE**  
The Myths of Churchill's War  
Gordon Corrigan  
Orion Books

Gordon Corrigan's *Mud, Blood and Poppycock* overturned the myths that surround the First World War. Now he challenges our assumptions about the Second World War in this controversial caustic narrative that exposes just how close Britain came to losing.

He reveals how Winston Churchill bears a heavy responsibility for the state of our forces in 1939, and how his interference in military operations caused a string of disasters. The



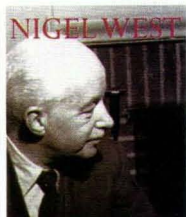
reputations of some of our most famous generals are also overturned: above all, Montgomery, whose post-war stature owes more to his skill with a pen than talent for command. But this is not just a story of personalities. Gordon Corrigan investigates how the British, who had the biggest and best army in the world in 1918, managed to forget everything they had learned in just twenty years.

The British invented the tank, but in 1940 it was the Germans who showed the world how to use them. After we avoided defeat, by the slimmest of margins, it was a very long haul to defeat Hitler's army, and one in which the Russians would ultimately bear the heaviest burden.

A reassessment of Britain's War, from the policy decisions in the 1920s to the great battles and campaigns of 1939-45. Hardback 493pp

Available from Eye Spy  
Ref: ES/1148 £22.99 \$48.00

**THE GUY LIDDELL DIARIES**  
Vol I 1939-1942



THE GUY LIDDELL  
DIARIES Vol. I: 1939-1942  
MI5'S DIRECTOR OF COUNTER-ESPIONAGE IN WORLD WAR TWO

Available from  
Eye Spy  
Ref: ES/1154  
£27.50 \$55.00

MI5's Director of Counter-Espionage in World War Two - Edited by Nigel West Routledge

Wallflowers is the codename given to one of MI5's most treasured possessions, the daily journal dictated from August 1939 to June 1945 by the Security Service Director of Counter-Espionage, Guy Liddell, to his secretary, Margo Huggins. The document was considered so highly classified that it was retained in the safe of successive 'D-Gs', and special permission was required to read it. Liddell was one of three brothers who all won the Military Cross during the First World War and subsequently joined MI5. He initially first served in the Metropolitan Police Special Branch at Scotland Yard, dealing primarily with cases of Soviet espionage, until he was transferred to MI5 in 1931. His social connections proved important because in 1940 he employed Anthony Blunt as his personal assistant and became a close friend of both Guy Burgess and Victor Rothschild, and was acquainted with Kim Philby. Despite these links, when Liddell retired from the Security Service in 1952 he was appointed security adviser to the Atomic Energy Commission, an extremely sensitive post following the conviction of the physicist Klaus Fuchs two years earlier. No other member of the Security Service is known to have maintained a diary and the twelve volumes of this journal represents a unique record of the events and personalities of the period, a veritable tour d'horizon of the entire subject. As Director, B Division, Liddell supervised all the major pre-war and wartime espionage investigations, maintained a watch on suspected pro-Nazis and laid the foundations of the famous 'double cross system' of enemy double agents. He was unquestionably one of the most reclusive and remarkable men of his generation, and a legend within his own organisation.

Order both volumes and save: Ref: ES/1156 £50.00 \$100.00



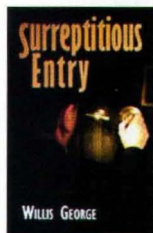
**THE GUY LIDDELL DIARIES**  
Vol II 1942-1945



THE GUY LIDDELL  
DIARIES Vol. II: 1942-1945  
MI5'S DIRECTOR OF COUNTER-ESPIONAGE IN WORLD WAR TWO

Available from  
Eye Spy  
Ref: ES/1155  
£27.50 \$55.00

**SURREPTITIOUS ENTRY**  
by Willis George  
Paladin Press



Written by one of the pioneers of clandestine spy tradecraft, this book is a fascinating look at government breaking-and-entering operations, including lock picking and safecracking. Educational Only. Softcover. Illustrated 208pp

Available from Eye Spy  
Ref: ES/1151 £25.00 \$30.00

**LAYMANS GUIDE TO ELECTRONIC EAVESDROPPING**  
How It's Done and Simple Ways to Prevent It by Tom Larsen  
Paladin Press

Phone lines, video cameras and room bugs are just a few of the tools nosy neighbours, angry spouses, private investigators and even the government can use to get the goods on you. This book will show you some simple, inexpensive ways to foil their efforts right now! Softcover. Illustrated. 112 pp

Available from Eye Spy  
Ref: ES/1006 £18.00 \$22.50

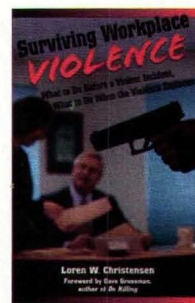
**SURVIVING WORKPLACE VIOLENCE: WHAT TO DO**  
by Loren Christensen  
Paladin Press

Do you work with someone who is unusually angry, antisocial, quick to take offence?

- How to recognise the warning signs in a co-workers behaviour that typically precede a violent act
- How to monitor suspect workers and interact with them on a daily basis
- How to analyse your immediate workspace and your overall work environment beforehand for escape routes, hiding places and barricade positions
- What to expect in an actual incident: gunfire, screams, disbelief and panic
- How to react quickly, decisively and safely when violence explodes
- Making the decision to fight back when you can't escape or hide, and how to best neutralize an attacker whether he is armed with a gun, knife or other weapon

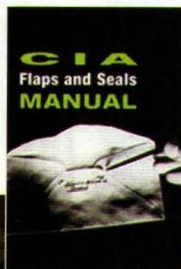
*Surviving Workplace Violence* answers the hard questions that company directives, magazine articles and other books leave out: exactly what you should do before a violent incident and what you should do if violence ever explodes where you work.

Loren Christensen began his law enforcement career in 1967 when he served in the army as a military policeman in the United States and in Vietnam. Softcover. 120pp.



Available from Eye Spy  
Ref: ES/1017 £19.99 \$20.00

**CIA FLAPS AND SEALS MANUAL Tradecraft Paladin**



This authentic manual reprint documents classic spy tradecraft used by the CIA and FBI to surreptitiously open and read suspects' mail. Chapters cover arranging the work area; selecting proper opening tools; opening mail with the dry, wet, and steam methods; defeating wax seals; resealing to cover one's tracks; detecting traps; examining received mail; and more.

This fascinating booklet is a must for historians, spy buffs, and anyone interested in the shadowy arts of espionage. Softcover. Illustrated 56pp

Available from  
Eye Spy  
Ref: ES/1147  
£13.99 \$16.00

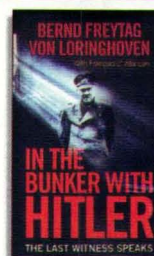
**IN THE BUNKER WITH HITLER**  
The Last Witness Speaks  
Bernd Freytag Von Loringhoven  
Orion Press

Originally published in France in March as *DANS LE BUNKER DE HITLER*, this is the story of a young German officer who not only survived Stalingrad and another year on the Russian Front, but made it out of Hitler's bunker to surrender to the British. He was ADC to the Hitler's last two commanders-in-chief, and the link between Hitler's Berlin bunker and the army's headquarters. He briefed Hitler on the deteriorating military situation and, at the same time, tried to help his friends arrested in the wake of the assassination attempt on Hitler in July 1944. Von Loringhoven spent the last weeks of the war underground with Hitler after Berlin

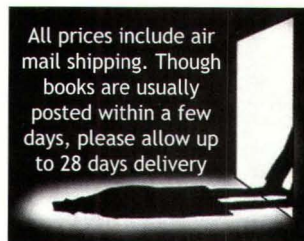
was surrounded, but escaped with two other officers to avoid falling into Russian hands. Hardback 207pp

Available from  
Eye Spy

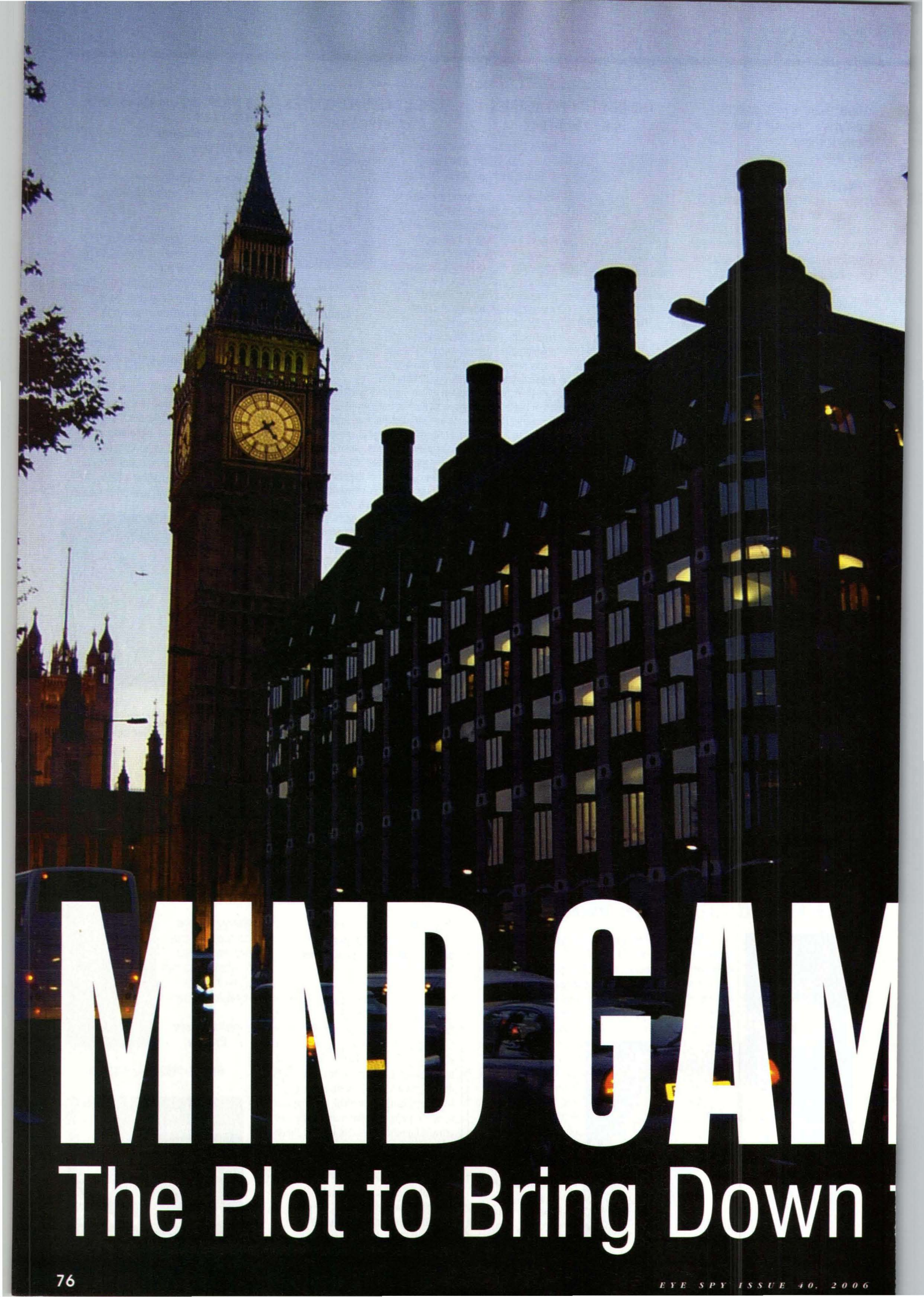
Ref: ES/1153 £14.99 \$30.00



All prices include air shipping. Though books are usually posted within a few days, please allow up to 28 days delivery







# MIND GAM

The Plot to Bring Down t



British Prime Minister Harold Wilson -  
some suspected he was a communist spy



**W**hen MI5 renegade Peter Wright (below) wrote about a plot by the intelligence service to force the resignation of British Prime Minister Harold Wilson, the public were astonished, the media fascinated, and the Security Service silent. Wright's book - *Spycatcher* was banned in the UK though the revelations inside soon reached the shores of Britain with lightning speed. Many political and intelligence experts rejected the allegations, and



even those who suspected some aspects of the story were true, called it an "exaggeration of facts." Now new evidence about the affair has again surfaced in a BBC drama documentary.

Broadcast in March 2006, *The Plot Against Harold Wilson* showed that far from being a 'flight of fancy', elements in the 'Establishment' and MI5 genuinely believed Harold Wilson, a staunch pipe-smoking socialist from Yorkshire, who never wavered from his working class upbringing, was considered a threat to the UK.

When Wilson first became premier in 1964, it was a time of Cold War paranoia. The Soviet Union was at its most menacing, and by the time he had finished his second stint in Downing Street in 1976, the trade union movement in Britain threatened to overwhelm Parliament with its power.

There was 'corridor' talk of Wilson being a communist sympathiser, though some in MI5 even dared to believe he was more than just a close ally of Moscow - he was a 'KGB asset'. According to information presented by the writers of the documentary, Britain was on the brink of a military coup - amazingly supported by The Royal Family. Absurd? Perhaps, but a number of parties close to Wilson at the time have parted with information that paints a very dark picture indeed.

BBC journalist Barrie Penrose interviewed Harold Wilson shortly before he resigned in 1976. He explained: "Our establishment, from the intelligence services down to parts of Fleet Street, were paranoid about the threat of communism. So paranoid it seems, they were prepared to believe a prime minister of Britain was an active Soviet spy."

By the mid-1970s those same Cold War tensions which Wilson had to cope with when he first entered Downing Street, were as frosty as ever. The leftwing unions had brought Britain to a virtual standstill - three days working weeks were commonplace, power cuts wrecked factories and inflation was running at ridiculous levels. Wilson was under attack and a disinformation campaign did not help. There were allegations of secret deals involving diamonds (Wilson supposedly received £1 million of precious South African stones), he allegedly backed IRA terrorists, and then he was accused of having an illicit affair with his political secretary, Marcia Williams (now Baroness Falkender). None of the stories were true, but by now Wilson's health was said to be suffering. The premier was adamant that his telephone was tapped, and when five members of his staff had their houses broken into, Wilson believed he had become an Establishment target.



The Berlin Wall

# ES?

# e British Government



# INTERNATIONAL CONFERENCE

Post-war intelligence, intelligence after 9/11,  
the future of intelligence

Conference at Christ Church,  
University of Oxford 2-8 September 2006

The conference brings together authors, experts and  
intelligence practitioners of international standing and  
examines the evolution of intelligence, espionage and  
deception across more than half a century since the end  
of World War II

The History of Intelligence, from 1945 to the end  
of the Cold War; The Present State of Intelligence,  
up to and beyond 9/11 and 7/7; and the Future of  
Intelligence: the new uncertain complexities we face in  
the 21st Century

For more information, brochure and booking form, please write:  
Alexandra Webb, Conference Administrator,  
The Steward's Office, Christ Church, Oxford, OX1 1DP

Tel: +44 (0)1865 276174 Fax: +(0)1865 286328  
Email: [Conflict@chch.ox.ac.uk](mailto:Conflict@chch.ox.ac.uk)



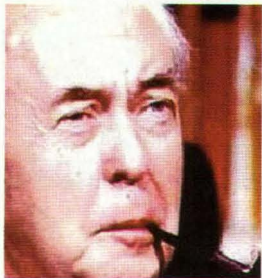
Speakers include: Professor  
Richard Aldrich, Chapman  
Pincher, Professor  
Christopher Bellamy, Dr  
David Khan, Nigel West, Bill  
Duff, Dr Stevyn Gibson, Dr  
Michael Goodman, Mark  
Seaman, Major R.A.M.  
Seegar, Dr Stephen J  
Weiss, Amir Taheri, Baron-  
ess Daphne Park...  
Full speaker biography  
[www.eyespyimag.com](http://www.eyespyimag.com)



The Conference is  
organised by Christ  
Church, a founder  
member of the Oxford  
Consortium and an  
Investor in People  
organisation

## Spies, Lies & Intelligence

### THE WILSON PLOT



Against this backdrop, Wilson believed a  
coup was being planned, and the British  
Army "might not come to his aid" - even  
forces just a few miles away from Down-  
ing Street itself.

#### SECRET RECORDINGS

*The Plot Against Harold Wilson* is  
based upon a number of covertly taped  
conversations made in 1976 by Penrose  
and his colleague Roger Courtiour with  
the prime minister. "Wilson spoke darkly  
of two military coups which he said had  
been planned to overthrow his govern-  
ment in the late 1960s and in the mid  
1970s," said Penrose. "Both were said to  
involve high-ranking elements in the  
British Army, eager to see the back of  
Labour governments. Both involved a  
member of the Royal Family - Prince  
Louis Mountbatten."

According to those close to the  
coup, Lord Mountbatten had been  
chosen as an interim prime minister.

"Unbeknown to Wilson, Courtiour and I  
secretly recorded many of our meetings  
with him, almost always conducted at his  
Georgian house at 5 Lord North Street,  
close to the House of Commons."

Penrose told the BBC's *Radio Times*.  
"The cumbersome machine was smuggled  
into his study in a briefcase carried by  
Courtiour. Over a period of nine months  
we accumulated hours of tape recordings.  
Those tapes have, since then, remained  
untouched in the loft of my Kent home  
and at Courtiour's London home."

Wilson was frank in his discussions and  
believed Fleet Street (where many of  
Britain's leading newspapers were once  
sited) was assisting shadowy forces.  
When they first met Wilson he told them:  
"Occasionally when we meet I might tell  
you to go to the Charing Cross Road and  
kick a blind man standing on the corner.  
That blind man may tell you something...  
lead you somewhere."

Whether the 'blind man' ever existed or  
not, the journalists were never advised

to travel to this area of London, but his  
deep mistrust of MI5 was obvious. He  
told them the Security Service were



Main picture: Buckingham Palace. Inset:  
Harold Wilson believed even troops based  
in London would not come to his rescue





Lord Mountbatten

"feeding" the press with false information, in particular about his alleged affair and links to Moscow.

In one of the recordings, Wilson explains: "I am not certain that for the last

eight months when I was prime minister I knew what was happening, fully, in security."

Baroness Falkender believed a coup was imminent and told the journalists that the prime minister and his cabinet would be arrested. As the black propaganda continued Wilson feared that the SAS would lead an assault on Downing Street. Just before the secret meetings ended, the prime minister warned Penrose and Courtiour to be "very careful."

These are extraordinary claims, but seemingly only support Harold Wilson's deepest fears. However, Brian Crozier, a former MI5 employee said senior army officers were involved in the plot, and that Lord Mountbatten, the last Viceroy of India and uncle of Prince Charles, revered by the public, would act as a stabilising influence until a new premier had been installed.

• Lord Mountbatten was killed by the IRA in August 1979. A bomb blast destroyed his boat off the coast of Donegal in the Irish Republic.



# SPECIAL READER OFFER

SAVE  
£100.00  
(\$150.00)



WAS £295.00  
NOW JUST  
£195.00!

## EYE SPY'S FAMOUS 'SPY PHONE'

This is a very serious and powerful surveillance device that allows the operator to listen in to a conversation from anywhere in the world. The phone looks and operates like any ordinary mobile-phone, however, by dialling its number you can monitor any conversation or sound that is within range of its highly impressive and advanced internal microphone.

The special microphone can detect the quietest of whispers. The unit can be taken into meetings or any environment, allowing colleagues thousands of miles away to listen in. Similarly, simply leave the phone at a location and dial up whenever you need to listen. All prices include p & p (shipping)

Order Code: LS-ENIGMA UK £195.00 USA \$349.00 ROW £210.00

With microphone attachment for vehicle use - please add  
UK £12.00 USA \$20.00 ROW £15.00

Please note - offer ends 1 June 2006!

## QUALITY EYE SPY BINDERS



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

Order Ref: ES/099

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

Please use order form  
on page 82



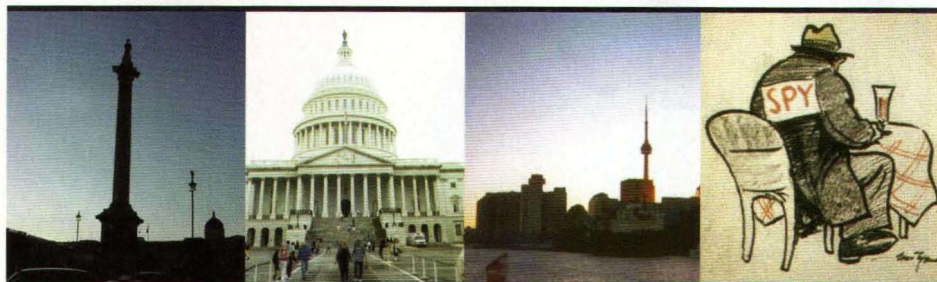


# • EYE SPY CLASSIFIED •

## SMALL CLASSIFIEDS

**INTERNATIONAL, CORPORATE, PRIVATE,  
PROFESSIONAL, SURVEILLANCE, TRAINING  
AND SECURITY ADVERTISING:**

**UK: 01756 770199 USA TOLL FREE 877 309 9243**



Eye Spy Intelligence Magazine Classifieds. All inserts appear in both USA, UK and Worldwide editions. Eye Spy Publishing Ltd reserve the right to refuse any advert without giving a reason for such a refusal. For a full media kit and details of all our excellent rates and special packages, please write to our USA, UK or Canadian address.

Similarly, you can e-mail your advert to us at: [advert@eyespymag.com](mailto:advert@eyespymag.com)

Payment must be enclosed with advert.

**Monies payable 'Eye Spy Publishing Ltd'**

Please do not send cash for goods when responding to advertisers.

*Eye Spy cannot be held responsible for delays in receiving goods from advertisers.*

**JUST 50P OR 75C A WORD**

### UNITED STATES OF AMERICA

Eye Spy International, Empire State Building, 350 Fifth Ave, Suite 3304-22H, New York, NY 10118-0069, United States of America

### CANADA

Eye Spy Canadian Bureau  
P.O. Box 153, Port Perry,  
Ontario, Canada, L9L 1A3

### UK, EUROPE, AUSTRALIA, REST OF WORLD

Eye Spy Intelligence Magazine, (Classified),  
P. O. Box 10, Skipton,  
North Yorkshire, BD23 5US, England

## SMALL CLASSIFIEDS

**FREE SAMPLE:** Special wafers - bend them, fold them, eat them, soak them - send \$2.00 to SOCIETY, PO Box 23321, Santa Barbara, CA, 93121, USA

**EYE SPY MAGAZINE:** We have a large number of readers urgently seeking issues 1, 6, 7 and 36. If you can assist, please telephone: 01756 770199

# Professional Services

## ISS TRAINING LTD

The World's Premier  
Surveillance Training Courses

Peter Jenkins - author of:  
**ADVANCED SURVEILLANCE**



Tel. UK 01423 712265

**Want To develop a Career In International VIP Protection ?**



I.S.A can provide the Training

**REAL VIP PROTECTION TRAINING**  
[www.SecurityAcademy.com](http://www.SecurityAcademy.com)



CALL - Israel +972 9 9500969 USA +1 2024703189 UK +44 2075588523

**To be the best, train with the best !**

**ijet** TRAVEL RISK MANAGEMENT

Keeping you safe, healthy and productive.

[www.ijet.com](http://www.ijet.com)

## POWER PUNCHING

**Revealed, The Quick And Easy Way To**



Double the power and speed of your punches in 90 days or less - Guaranteed! Finally! Highly respected renowned self defence expert, John Brawn, breaks his 15-year silence to teach you the secret of his incredible punching power so you can quickly and easily learn how to land a flurry of lightning-fast punches with devastating power to completely obliterate your opponent.

**100 Day -  
100% Money  
Back  
Guarantee!**

A new DVD you can view in the comfort of your own home will teach you exactly the correct form and technique while you watch!

For details of Power Punches Volume One, write to:- John Brawn, 21 St. Patrick's Terrace, Westport, Co. Mayo, Ireland

or visit:-

[www.powerpunches.com](http://www.powerpunches.com)



**WAYNE BRIDGES INVESTIGATIONS**  
CALIFORNIA

(213) 304-9830 (213) 304-5983

International 011-61-39-818-4214

LICENSED / CIVIL / CRIMINAL MATTERS  
WORLDWIDE PROFESSIONAL SERVICES

**Cerebus Systems**

[cerebus-systems.com](http://cerebus-systems.com)

**BRIXMIS  
ASSOCIATION**

[www.brixmis.co.uk](http://www.brixmis.co.uk)





## International Bodyguard Association

The oldest and largest bodyguard association with sites of protective service and education worldwide



### WE OFFER THE FOLLOWING COURSES:

Bodyguard Master Class, Specialist Protective Escort, Protective Driving, Bodyguard Tactical Firearms, Defence and Restraint Tactics, Electronic Surveillance Devices (ESD) Search, Improvised Explosive Devices (IED) Search, Bodyguard Counter Sniper, Bodyguard Paramedicine, Private Yacht Protection, Private Aircraft Protection.



Contact: Office of the Director General, International Bodyguard Association, Borrmount Manor, Borrmount, Enniscorthy, Co. Wexford, Republic of Ireland

Tel. + 353 53 30821 Fax. + 353 53 30822  
www.ibabodyguards.com

**NIGHT PALM 4**  
Multi-Functional Torch  
AVAILABLE FROM EYE SPY

Ref: ES/NPALM4 UK: £15.45  
USA: \$27.50 EUROPE: £17.00  
ROW: £18.50  
(prices include p & p)  
Use order form on page 82

**THE SPYCRAFT MANUAL**  
THE INSIDER'S GUIDE TO ESPIONAGE TECHNIQUES

FOREWORD BY  
RICHARD TOMLINSON  
BARRY DAVIES, B.E.M.  
SPY SCHOOL INSTRUCTOR

AVAILABLE FROM EYE SPY  
Ref: ES/984 £17.99 \$45.00

## PPA INTERNATIONAL

### TRAIN AS A CLOSE PROTECTION OPERATIVE

Learn the skills necessary to work in high-risk areas



PPA INTERNATIONAL



#### SPECIALISED CPO COURSES:

- 3-Week Advanced CPO Course
- 6-Week Specialised CPO and Security Consultant Course
- 4-Day Tactical Firearms/Advanced First Aid Course
- Live Firearm Training with a variety of Contact Drills combined with First Aid Training

PPA instructors are former officers and head instructors for Australian SAS, US Marine Recon, UN Peacekeeping Forces and Danish Recon. All PPA instructors have first-hand experience of working in high-risk conflict areas. The experience and training you will receive will help you protect, survive and find job opportunities

Visit PPA's website for additional information on courses and announcements

TO BE  
THE BEST -  
LEARN FROM  
THE BEST

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

Tel. +45 47 77 17 36

is your conversation safe?

**YOU TALK, WHO IS REALLY LISTENING?**

The Enigma T301 is a totally secure, fully upgradeable mobile phone that uses military-level encryption to enable unbreachable communication with other Enigma users via all standard GSM networks.

*enigma*

To find out more call:  
**+44(0)20 8916 2180**  
fax +44(0)20 8916 2181  
email info@tcominternational.co.uk

Enhancing  
Your  
Performance

Continuing Education  
Available Today

Visit  
www.Spy-Ops.com to receive  
your free Training Brief on  
Corporate Espionage and  
learn about our exciting New  
Offerings.



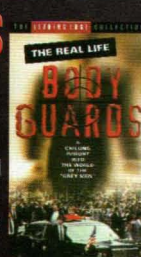
**BODYGUARDS**  
THE VIDEO (PAL ONLY)

A chilling insight into the world of the professional bodyguard - the flesh and blood that stand between the world's most powerful leaders and their would-be assassins.

These are the real 'grey men' - Eye Spy

PAL VHS Ref: ES/20  
UK £8.49 EUR £9.99  
ROW £10.99 USA \$20.00  
60 minute documentary

US readers note - this is not NTSC. Available from Eye Spy - use form on page 82



**technolytics**

Technology  
for  
Intelligence

A new technology revolution is coming!

Will you lead...  
follow...  
or be pushed aside?

www.technolytics.com



# FLIGHT 93

CONTINUED FROM PAGE 59

COURTESY: USAF

door and in all probability gained access. In this confusion the hijackers began swinging the aircraft violently to try and unbalance the passengers. They lost control and the aeroplane flipped over.

The tapes are as revealing as they are frightening. Some passengers, presumably via cell phones or from the hijackers themselves, knew the World Trade Center had been attacked. It was at this point a degree of realisation overwhelmed everyone on board. It was no ordinary hijacking. "There is absolutely no doubt that through their heroic actions still more carnage and catastrophe was prevented," said Richard Ben-Veniste, a member of the independent commission that investigated the attacks. The commission concluded that the actions of passengers on board Flight 93 stopped an attack that was aimed at Washington.

Jury members, who must decide whether Moussaoui should receive the death penalty or life in prison, were shown a computer simulation played on monitors throughout the courtroom. The large airliner moved violently through the sky during the struggle. Data analysis showed the hijackers tried to cut off the

Captain Jason Dahl, United Airlines Flight 93 dreamed of flying an F-16 fighter jet, but he never lived to get his chance. The Colorado Air National Guard's 140th Wing gave his wife, Sandra, the honour. Here, Sandra Dahl shows some items that she carried in her pocket during her F-16 flight, including photos of her husband in his pilot uniform, and an 'ace of spades' that she found in his flight suit

oxygen as passengers banged on the cockpit door. One of the hijackers is heard screaming as Flight 93 entered its final death roll. Seconds later the cockpit recording went dead.

For the jury and media listening to the events unfold inside the District Court in Alexandria, it was a traumatic time. Lorne

Lyles, a police officer from Florida, whose wife, CeeCee, was a flight attendant on Flight 93, telephoned twice during the incident. Asleep at the time, Lyles had just finished a long night shift and had rolled over and gone back to sleep. Seven days after the incident he heard the message on his voice mail. "Hi, baby... you have to listen to me very carefully. I'm on a plane that has been hijacked... I'm trying to be calm."

Left: Artist's impression of the Flight 93 memorial. Families trying to raise the \$30 million needed to build the monument were given a boost when Universal Pictures said it was giving 10 per cent of all box office revenue collected from its movie - 'United 93', which opened on 28 April 2006



## OFFICIAL EYE SPY ORDER FORM 2006

| 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 (USA)



### CANADA

Eye Spy Magazine, Canadian Bureau  
P.O. Box 153, Port Perry, Ontario, Canada, L9L 1A3  
Or Telephone 01756 770199 (UK)

WE NOW ACCEPT ORDERS VIA PAY PAL [eyespy@eyespyimag.com](mailto:eyespy@eyespyimag.com)

Sorry, at present we do not take American Express

Don't cut the form and spoil your magazine! Handwritten orders accepted. Please write clearly



# 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



Henry Hockelmer  
legal editor



MARK IAN BIRDSALL  
editor



Lynn Hodgson  
Canadian editor



Glenmore Trehear Harvey  
associate editor



Jim Shortt  
military consultant



Peter Jenkins  
surveillance editor



Spiros Kopitsos  
Greece editor



Donald Napier  
intel news



Kevin Coleman  
consultant

Director of International Corporate Affairs: Deborah McDonald  
Copy Editor: Ian Cole  
Senior Photo Consultant: Steve McManus - Law Enforcement Picture Library



Nick Fielding  
senior intelligence consultant



David Bickford  
senior intelligence consultant

EYE SPY MAGAZINE AVAILABLE IN 36 COUNTRIES



EYE SPY welcomes articles, photographs, case files, special reports, documents and newscippings 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.

Eye Spy Magazine: Legal Counsel -  
Hangley Aronchick Segal & Pudlin, One Logan Square,  
27th Floor, Philadelphia, PA 19103, USA

subscriptions

|                                   |                    |
|-----------------------------------|--------------------|
| united kingdom                    | \$25.00            |
| united states of america          | \$48.00            |
| europa                            | \$30.00            |
| Canada                            | C\$60.00 (\$30.00) |
| australia/middle east/asia/africa | \$32.00            |

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.

curtis

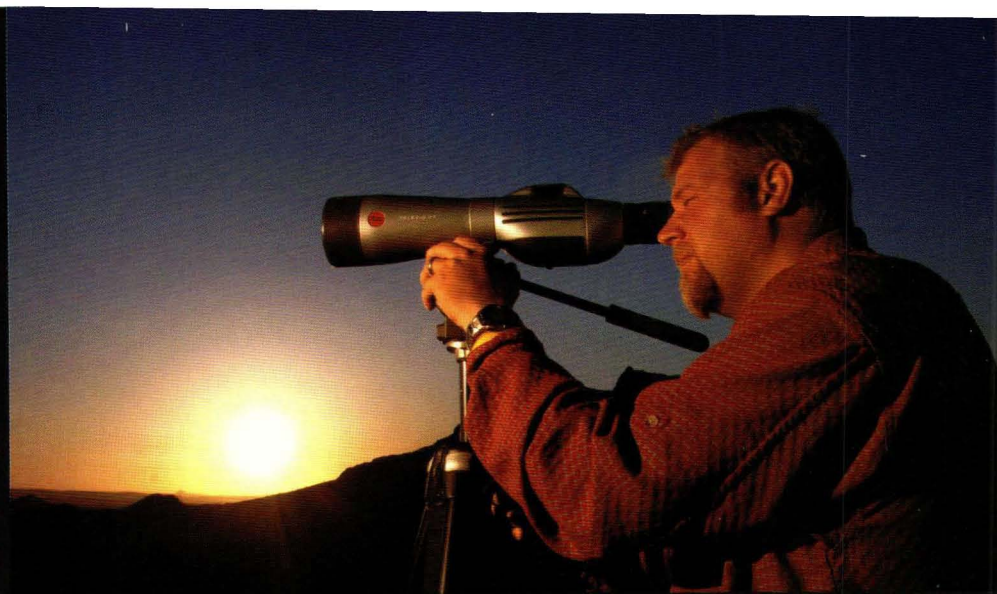
NORTH AMERICA distribution

UNITED STATES OF AMERICA & CANADA -  
Curtis Circulation Company

magazine

UK·EUROPE·ROW distribution

UK, Europe, Australasia, Rest of World  
Imagine: UK 0845A 612 0094



## COMING SOON IN EYE SPY

ISSUE 41 ON SALE 30 JUNE 2006

- THE ART OF DISGUISE
- INTERCEPTING E-MAILS AND PHONE CALLS
- SPY TIPS FOR HOME SECURITY
- TRADECRAFT - CATCHING INTRUDERS
- SPIES AND DISINFORMATION
- USING INTELLIGENCE CORRECTLY
- TRACKING TERRORIST MONIES
- LIE DETECTORS - USEFUL OR USELESS TOOL?
- BALLISTICS AND FORENSICS
- NOTES FROM THE CODE BREAKERS



*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,

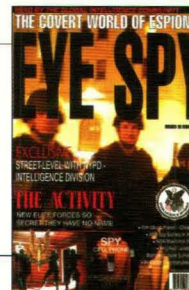
Please reserve/deliver\* a copy of EYESPY on publication, starting with the next available issue

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 WEB SITE

FOR ALL YOUR INTELLIGENCE REQUIREMENTS

# 24 HOURS A DAY



- SUBSCRIPTIONS
- EYE SPY ARCHIVES
- INTELLIGENCE RESOURCES
- ESPIONAGE CASE FILES
- SURVEILLANCE DEVICES
- PROFESSIONAL EQUIPMENT
- INTELLIGENCE BOOKS
- TRADE SECURITY BOOKS
- BACK ISSUES
- 24 HOUR NEWS SERVICE
- SECURITY ADVICE
- SPECIAL OFFERS
- DISCUSSION BOARD
- PHOTO GALLERY
- PROFESSIONAL LINKS

TO SUBSCRIBE

UK CALL 01756 770199 (standard BT rates)

USA/CANADA 877 309 9243 (Toll Free)

REST OF WORLD + 44 1756 770199

# EYE SPY

[www.eyespymag.com](http://www.eyespymag.com)