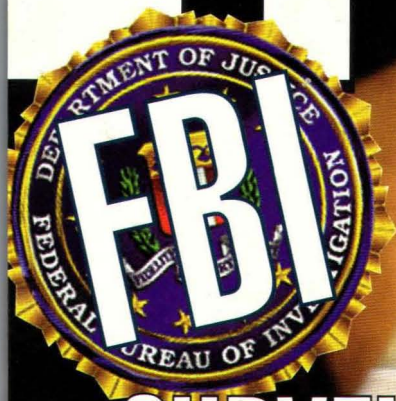


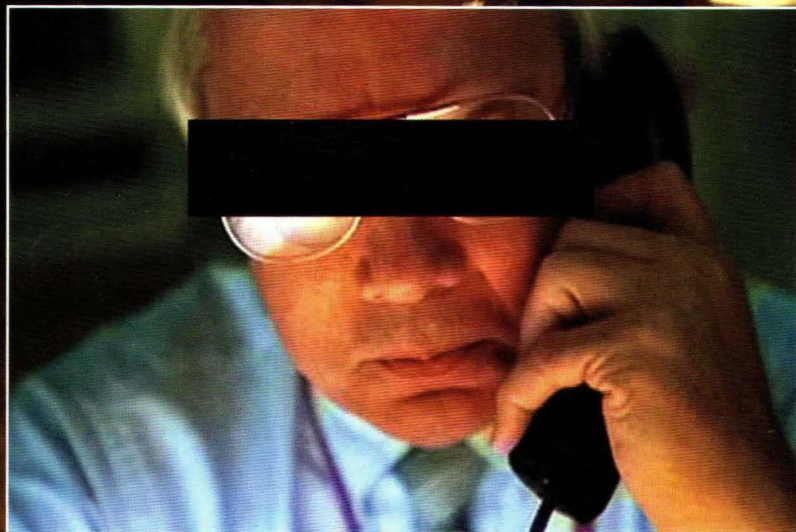
READ BY THE GLOBAL INTELLIGENCE COMMUNITY
THE COVERT WORLD OF ESPIONAGE

EYE SPY

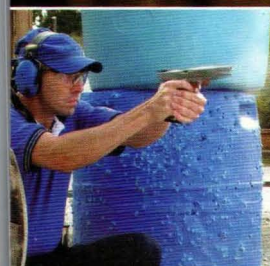


SURVEILLANCE TIPS

**MI6
AND IRAQ**



HOSTILE ENVIRONMENT TRAINING



**Iran - Out of Time?
NSA Eavesdropping
Profiling a Terrorist**

VOLUME V NO. 38 2006 USA \$5.99 CANADA C\$7.99

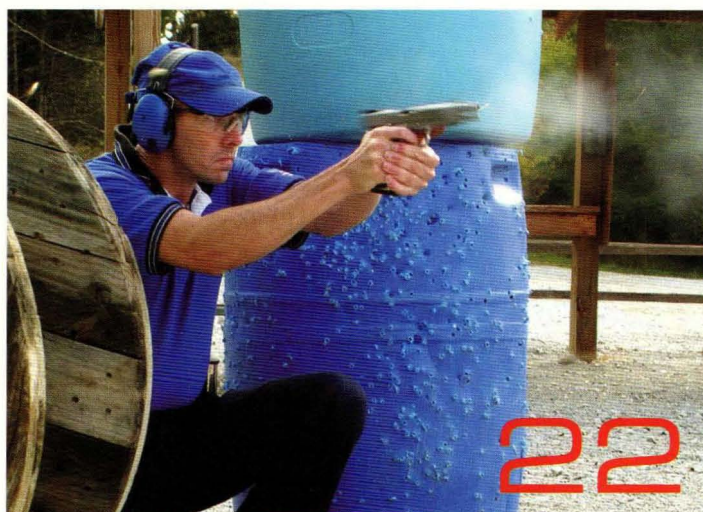


38 >

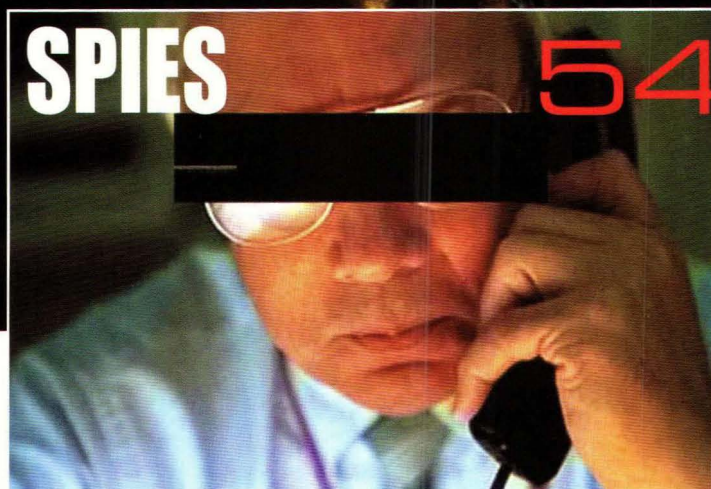
SURVEILLANCE - FBI STYLE 8

Conducting Surveillance
Operations - How to Get the
Most Out of Them

HOSTILE ENVIRONMENT SURVIVAL



SPIES 54



Should their identities always be protected?

WHAT WENT WRONG WITH MI6 ON IRAQ

57

The inside story
that reveals
why MI6 got it
so wrong on
Saddam's WMD



EYE SPY

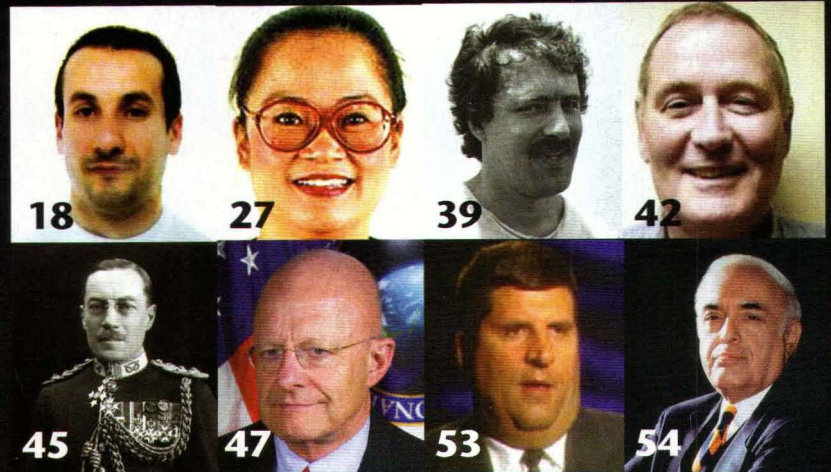
CONTENTS

- 14 **The Ghost**
A former spy wanted by the Spanish authorities who died in 1998, has suddenly emerged from the grave
- 18 **End of the Identity Man**
An Algerian al-Qaida suspect known as the 'identity man' was jailed in Belfast - police still do not know his real name
- 27 **Agent Parlour Maid**
A Chinese FBI informant once charged with espionage has been found not guilty by a court
- 30 **Intelligence Failure?**
A UK Board of Inquiry says an attack on a British helicopter in Iraq could have been prevented if intelligence had not been compartmentalised
- 36 **The Briefing Room**
A series of official photographs showing how banned weapons and artifacts are being concealed
- 39 **MI6 and France DGSE in Spy Wars**
Newly released documents show France created a plan to blame MI6 on the sinking of the Greenpeace vessel Rainbow Warrior
- 42 **FBI Still Searching for Anthrax Man**
No-one has been charged with the sending of anthrax-laced letters in 2001... is the FBI any nearer to finding the culprit?
- 44 **MI5 - Hall of Mirrors**
In a remarkable move, Britain's Security Service has uploaded on its web site photographs and brief biographies of all its former Director-Generals
- 50 **Secret Signals - NSA Playing at Home**
A major controversy has erupted as the NSA eavesdrops on US-based telephones
- 64 **Iran - Out of Time?**
Intelligence watchers believe an attack on Iran's burgeoning nuclear industry is now inevitable
- 68 **Profiling a Terrorist**
Reader interactive series on understanding intelligence. This feature explains how the security service perform terrorist profiling

32

Air Marshals take to the streets

VIPER SURVEILLANCE



MAKING NEWS IN EYE SPY:

- 18 Abbas Boutrou • 27 Katrina Leung • 39 Fernando Dopereira
- 42 Bob Stevens • 45 Vernon Kell
- 47 James Clapper • 53 Russell Tice • 54 Bob Novak

some inside features

4 Intelligence Briefings; 6 Intelligence Extra; 16 Trade Books;
48 Back issues; 63 Newspaper names MI6 Station Chief;
74 Undercover - Book Releases; 78 Product Review; 80 Eye Spy Classified

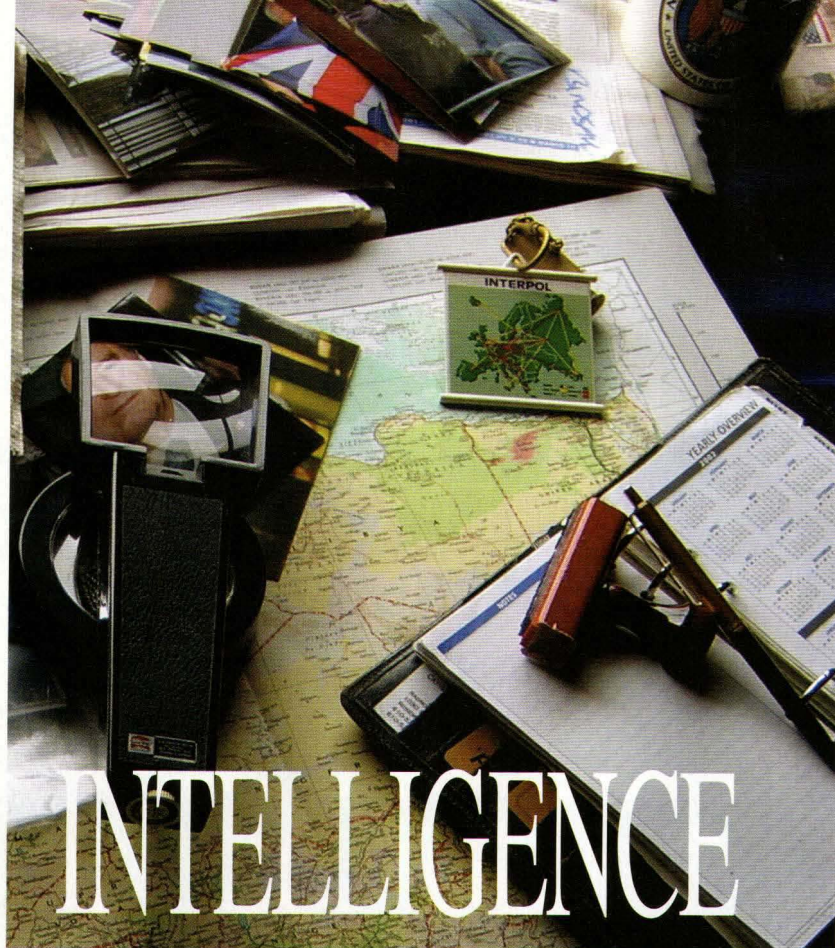


EYE SPY EDITORIAL

INTELLIGENCE SECRETS AND THE PUBLIC

Those working for an intelligence service, especially as one as secret as the NSA often find that the material they handle is highly classified and, at times, controversial. Most workers see the information as a product of their business and accept the need for secrecy. However, it seems leaks are becoming more prevalent and journalists can find themselves in possession of state secrets. The decision to publish or not is fraught with danger - not least because the information could be useful to an adversary. In recent months the controversy about the NSA tapping US landlines has reached the press. One primary source is a former NSA employee - sacked last summer. He claims the NSA acted illegally, but is this really his reason for "outing" a secret project? Probably not, and in any event, few members of the public would not be grateful if the operation prevented another terrorist attack on the scale of 9/11. It remains to be seen if the employee will be charged, but it would be futile to blame the media for printing his allegations. As the ranks of the intelligence services in the USA, UK and elsewhere are swelled by new recruits, it seems likely more leaks will occur. However, is it not strange that most leaks occur after an employee has been disciplined or dismissed? If they can't keep secrets, what on earth were they thinking of in the first place when they joined an industry where silence is paramount?

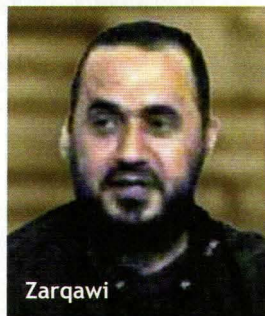




INTELLIGENCE

World's Most Wanted - Released - by Security Forces

Iraqi security forces reportedly caught terror leader Abu Musab al-Zarqawi but released him because they did not realise who he was. The Jordanian-born terrorist - head of al-Qaida in Iraq - is known to have murdered British hostage Ken Bigley, an engineer from Liverpool and numerous other foreign workers in Iraq. News of the security debacle was revealed by Iraq's Deputy Interior Minister, Hussein Kamal, who said al-Zarqawi was indeed in custody in 2005. He refused to provide further details. Though the report could not be confirmed, a US official said that American intelligence believed it was plausible.



Zarqawi

There have been several reports of missed opportunities to capture al-Zarqawi, including a raid in April 2005 by US troops acting on a tip-off from local informants that militants, reportedly including the terror leader, were hiding in a hospital in Ramadi. Al-Zarqawi narrowly escaped after an al-Qaida convoy was stopped in heavy traffic on a motorway in Iraq.

Al-Zarqawi played a pivotal role in the death of US aid worker Laurence Foley in Jordan in 2002. Since then his group has carried out several murders which have even been criticised by Osama bin-Laden. Jordan has sentenced al-Zarqawi to death in absentia and Washington has placed a \$25 million reward for his capture.

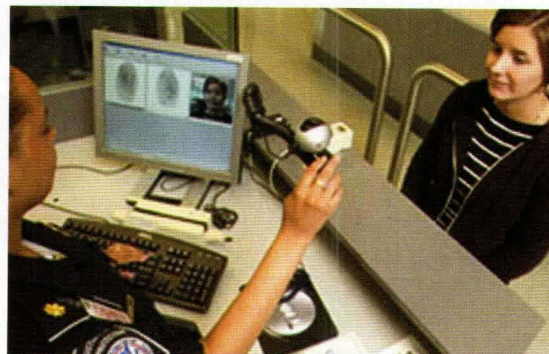
Madrid Bomb Planner Arrested

MADRID: Spain's security forces have arrested a "key member" of al-Qaida suspected of planning the escape routes used by the terrorists who blew up several trains near Madrid in 2004. In an Interior Ministry statement, the man was named as Omar Nakhcha, 23, the alleged ring-leader of two cells believed to have recruited men to fight in Iraq. Those cells were dismantled by police earlier in early January and 20 people arrested. The arrests followed a massive intelligence-led investigation assisted by Italian, French and Belgium anti-terrorist police. Some 200 people have now been arrested in connection with the atrocity that left 191 people dead.

US Biometric Security Enhanced

The Department of Homeland Security's US-VISIT programme has completed installation of biometric entry capabilities at 104 land border ports. Biometric entry capabilities are

comparing their biometric and biographic information against watch lists of terrorists, criminals, and immigration violators. Since January 2004, US-VISIT has processed more than 44 million visitors, which



COURTESY: DHS

A Customs and Border Protection agent reviews the electronic photo and fingerprints of a visitor

now deployed at all fixed ports of entry open to US-VISIT travellers.

US-VISIT is a continuum of security measures that collect biometric and biographic information from visitors at US visa-issuing posts upon their arrival and departure from US air, sea and land border ports. The programme enhances security by verifying each visitors' identity and by

makes the program the largest-scale application of biometrics in the world. Biometrics have enabled US-VISIT to intercept, at US ports of entry, more than 970 people with histories of criminal or immigration violations, including federal penitentiary escapees, convicted rapists, drug traffickers, individuals convicted of murder, and numerous immigration violators.



Moscow's Spy Numbers "Not Increasing"

Many of the West's intelligence services have reported a significant increase in Russian espionage activity, though Moscow itself claims this is not true. On 20 December 2005, as Russia's Foreign Intelligence Service celebrated its 85th anniversary, current director, Sergei Lebedev refuted suggestions that Russia has as many operational as it did during the Cold War. "This is not so. In comparison with that period, the Russian intelligence service has curtailed its presence

abroad and drastically reorganised its functioning," he said. A reference to its increased commitment in fighting terrorism.

Lebedev blamed Russia's enemies for providing the media with "negative reports" and said the covert disinformation programme was "probably paid for by those who do not want relations with Russia to continue to develop." He continued: "To my regret, it has become a rule to scare ordinary citizens abroad with Russian spies, who have allegedly made inroads

into all of the agencies. There have been instances of local counter-intelligence services deliberately exaggerating the Russian espionage threat to show their relevancy, enhance their staff or to secure more funds."

Lebedev refused to be drawn on the possibility that Moscow has created such spy rings as those known as the 'Cambridge Five'. Though he candidly advised journalists to ask his successor in 50 years time. He also rejected claims that Moscow still sees Washington and London as "adversaries"



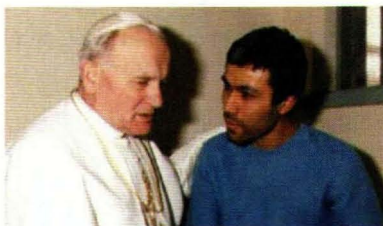
COURTESY: MOSCOW NEWS

and pointed to the new developing threat of terrorism as a global priority. "The special services of a number of European countries carried out a joint operation in November 2005 to arrest leaders and members of al-Qaida cells in Belgium, France, Italy and other states," he said. "Terrorism can be defeated only through joint efforts of all

countries, their special services, other state bodies, and international organisations. The Foreign Intelligence Service's cooperation with its foreign colleagues helps achieve greater results in the anti-terrorist fight. That is why we are committed to further strengthening of international cooperation in this area."

Agca - Failed Pope Assassin Released

ISTANBUL: The man who tried to kill Pope John Paul II on 13 May 1981, was released from a Turkish prison on 12 January 2006. A now grey-haired Mehmet Ali Agca, 48, left the prison and got into his lawyer's car amid a chaotic scene created by international media and about 50 nationalists who consider him a hero. One of Agca's supporters threw flowers onto the car as it drove away. After serving 20 years in prison in Italy following the attempted assassination in St. Peter's Square at the Vatican, was transferred to Turkey to serve time for the 1979 murder of Turkish left-wing newspaper editor Abdi Ipekci and the robbery of an Istanbul factory that year. Although Agca has served less than five years for Ipekci's murder, under Turkish law his time in prison in Italy counted.



Russian Intelligence Officials in UK to Study Tactics

BELFAST: A group of senior Russian security officials, including Mikhail Belousov, head of the FSB's operations coordination directorate for the North Caucasus Teymuraz Kaloyev, spent several days in Northern Ireland in January to study Britain's experience in fighting terrorism and organised crime. One of the group said: "We shared our experiences of working on cooperation between the armed forces and the police to organise the fight against terrorism. In addition, we met representatives of the Northern Ireland Police and the agency responsible for combating organised crime. The experiences of the structures responsible for combating money laundering and the return of illegally obtained funds were interesting," he said.

2003 Top Secret Report Warned of London Attack

Senior intelligence officials warned Downing Street two-years prior to the London bombings of July 2005, that the London Underground was "high" on al-Qaida 'wish list' of targets. A Top Secret 4-page document leaked to the media and prepared by the Joint Intelligence Committee (JIC), which effectively overseas all UK spying, noted that al-Qaida was specifically targeting the "London Tube."

Dated 2 April 2003, two years prior to the London attacks, the report was "signed off" by the heads of the UK's three primary intelligence agencies - MI6, MI5 and GCHQ. It is understood that some of the intelligence was gleaned from interrogations of Khalid Sheikh Mohammed, who was the terror group's primary planner before he was arrested.

Part of the report read: *The UK and its interests*

remain high in al-Qaida's priorities. Plans have been considered to attack Heathrow [Airport], the London Underground and other targets.

Other sections reveal MI6 is highly active in tracking al-Qaida across the globe, including Africa where a number of suspects are under surveillance. *We do not yet know the full nature of their activity, but they are planning attacks*

Mohammad Sidique Khan - MI5 decided he was not a threat



here... some have been questioned by the police.

Four of the failed 21 July 2005 bombers came from Africa, including Ethiopia, Eritrea and Somalia.

Pressure is now mounting on Downing Street to disclose the full report, especially after Prime Minister Tony Blair

refused to hold a public hearing into the attacks. MI5 admitted it lost track of 7 July terror leader Mohammad Sidique Khan whom it had under temporary surveillance prior to the attacks. He was not considered a threat based on his profiling and other information.



EYE SPY



INTERNATIONAL INTELLIGENCE EXTRA

NEW USA SPY CASE

COUPLE PROVIDED INTELLIGENCE ON US CUBAN COMMUNITY

The FBI has revealed details of what it said was a husband-and-wife spy team at Florida International University. According to intelligence sources, the couple could have been operating for decades.

Carlos M. Alvarez, 61, a Florida International University professor and his wife, Elsa, 55, an FIU counsellor, were accused of working as "covert agents" for Cuba. The couple allegedly used shortwave radios, numerical-code language and computer-encrypted files to forward information about Miami's resident Cuban community to senior Castro intelligence officers.

US Magistrate Judge Andrea Simonton even denied them bond before the trial on a charge of failing to register with the federal government as foreign agents. Apparently both Mr and Mrs Alvarez had admitted the charges to the FBI last summer. The govern-

ment believed that the couple could flee to Cuba if they were granted bail. "As a practical matter, these are people who admitted they were spying," Simonton said. "They would indeed return to Cuba, rather than face the consequences of their actions here." Their solicitors noted that they had not fled the USA even after admitting the charges. "There is not a scintilla of evidence that they contemplated leaving for Cuba," said one of the defence lawyers.

According to the FBI and federal prosecutors, the couple "transmitted information about Miami's exile community - including leading groups such as the Cuban American National Foundation and Brothers to the Rescue."

While it is likely the information does not pose a threat to the security of the United States, the couple apparently did supply details of an FBI employee who had once been



an FIU student of Carlos Alvarez.

Carlos Alvarez is an associate professor of educational leadership and policy studies at FIU who also does psychological screenings of police cadets for the city of Miami and Miami-Dade County police departments.

"They used their academic positions as covert covers to spy for the Cuban government," said Assistant US Attorney Brian Frazier. "They were living a lie." Frazier said Carlos Alvarez had spied for Cuba since 1977 and his wife since 1982. It is understood neither received payment for their activities but Cuba did forward monies for their

IMAGINATIVE LONDON COUNTER-TERRORISM ADVERTISING CAMPAIGN LAUNCHED

"Terrorists won't succeed if someone reports suspicious activity - and you are that someone"

That was the message of a four-week counter-terrorism advertising campaign launched by the UK's Metropolitan Police in January.

Peter Clarke, head of the Met's Anti-Terrorist

Branch said: "Everyone who lives in London, or visits the city for work or pleasure, has a role to play in making it as difficult as we can for terrorists to operate here. We can all help by being vigilant and aware

of what is happening around us. If it seems suspicious to you, please make that call.

"This publicity campaign is not a response to any specific threat, but I would urge the public to

continue to remain alert. We cannot afford to be complacent."

The campaign was intended to encourage people to have the confidence to trust their instincts and report any

suspicious bags, vehicles or behaviour to the police immediately by dialling 999. The posters were displayed on bus shelters, roadside sites and at train stations across the London, augmented by press

TERRORISTS WON'T SUCCEED IF SOMEONE REPORTS SUSPICIOUS ACTIVITY

YOU ARE THAT SOMEONE

CALL 0800 789 321 (ANTI-TERRORISM HOTLINE)

IF YOU SUSPECT IT REPORT IT

TERRORISTS WON'T SUCCEED IF SOMEONE REPORTS SUSPICIOUS ACTIVITY

YOU ARE THAT SOMEONE

CALL 0800 789 321 (ANTI-TERRORISM HOTLINE)

IF YOU SUSPECT IT REPORT IT

TERRORISTS WON'T SUCCEED IF SOMEONE REPORTS SUSPICIOUS ACTIVITY

YOU ARE THAT SOMEONE

CALL 0800 789 321 (ANTI-TERRORISM HOTLINE)

IF YOU SUSPECT IT REPORT IT

TERRORISTS WON'T SUCCEED IF SOMEONE REPORTS SUSPICIOUS ACTIVITY

YOU ARE THAT SOMEONE

CALL 0800 789 321 (ANTI-TERRORISM HOTLINE)

IF YOU SUSPECT IT REPORT IT

TERRORISTS WON'T SUCCEED IF SOMEONE REPORTS SUSPICIOUS ACTIVITY

YOU ARE THAT SOMEONE

CALL 0800 789 321 (ANTI-TERRORISM HOTLINE)

IF YOU SUSPECT IT REPORT IT

COURTESY: METROPOLITAN POLICE

expenses, including accommodation, travel and food.

The FBI were tipped-off about the couple who used the codewords David and Deborah, and placed under surveillance.

LOW-COST TECHNOLOGY

The couple used various low-tech methods to communicate

with handlers and colleagues in Cuba, Mexico and South America. An antenna in their garden provided the means to send signals. Other information was sent using an encrypted computer programme and ordinary mail via post boxes.

This has been the modus operandi for numerous Cuban spy rings in the USA.

FOR THE INTELLIGENCE RECORD



50% OF AMERICANS SUPPORT COVERT EAVESDROPPING WITHOUT WARRANT

WASHINGTON: A CNN/USA Today/Gallup poll of 1,003 adults found that 50 percent of those polled believe it's fine to place people suspected of having ties to terrorists abroad under electronic surveillance without first obtaining a warrant. Another 46 percent said the policy is wrong, and 4 percent said they had no opinion. President Bush has defended signing secret orders allowing the National Security Agency to intercept international communications by people in the United States who are suspected of having links to terrorist organisations.

FAMOUS SPY DIES IN USA

SAN FRANCISCO: Kurt Singer, born in Vienna died on 9 December, 2005, in Santa Barbara, California, aged 94. Singer was an anti-Nazi activist and spy during the Second World War whose dozens of books include works on espionage and biographies on subjects as diverse as Hitler's henchman Hermann Goering and the actor Danny Kaye. After fleeing to Stockholm he spied for both the United States and Sweden supplying valuable intelligence on Nazi Germany and later the Soviets.



M15 TO RECRUIT 200 ADDITIONAL COUNTER-TERRORIST OFFICERS

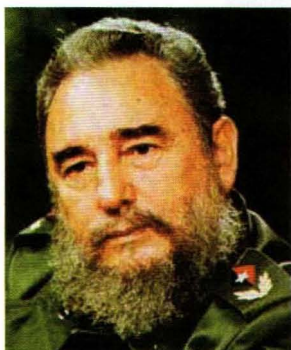
LONDON: The Security Service is to bolster its anti-terrorism capabilities by spending an injection of government money to recruit up to 200 additional anti-terrorism officers. By 2008, staff levels in M15 will have risen well above 3,500 with some 70-75% devoted to counter-terrorism operations. Many will be employed in surveillance roles as officials recognise the emerging threat from persons residing in the UK involved in terrorist activities.

1998 CUBAN SPY ADMISSION

The case of the Alvarez' surprises few intelligence watchers. In 1998, Fidel Castro admitted sending spies to the United States to gather information about what he called "terrorist activities" by anti-Cuban political groups, but Castro denied there were any attempts to spy on the US military or intelligence community.

In an interview with CNN's WorldView, Castro said: "Yes, we have sometimes dispatched Cuban citizens to the United States to infiltrate counterrevolutionary organisations, to inform us about activities that are of great interest to us."

"I think we have the right to do this," he said. "The United States has spies in industrial quantities."



Peter Clarke

adverts appearing in the major London newspapers. The campaign was also reinforced by a thought-provoking radio advertisement on London commercial radio stations.

ANTI-TERRORIST HOTLINE

The public are also being encouraged to contact the confidential anti-terrorist hotline on 0800 789321 if they have information about possible terrorist-related activity.

The police note: "Terrorists need places to live and to store equipment and materials. They need people to help them and may need transport in order to carry out their plans. They need to raise money, and may use fraudulent transactions to help fund their activities." Henceforth five cleverly constructed posters each containing a single image provided a visual clue.

Aimed at the general public and those working in particular professions, they encouraged people to report any suspicious activity. Three of these posters focus on the rental or sale of accommodation, garage and lock-up facilities, and of vehicles. Another poster encourages retail and bank staff to be aware of fraudulent transactions that may be linked to terrorist fund-raising and a fifth focuses on the need for vigilance within the river and marine environment.



EYE SPY

SURVEILLANCE FBI STYLE

Conducting Surveillance Operations - How to Get the Most Out of Them



By **JOHN T. NASON** - Special Agent Nason heads the FBI's Special Operations Group, Aviation and Surveillance Operations Section, Critical Incident Response Group

As the Hollywood detective sits in his four-door sedan, he downs numerous cups of coffee to stay awake and occasionally speaks into a two-way radio to other officers also maintaining the same stake-out ritual. Then, finally, in the pre-dawn hours, the villain emerges from the location, playing right into the hands of the seasoned and street-smart hero who tails him to where he commits a crime, takes a hostage, or retrieves some stashed contraband. Then, in action-packed style, the detective handles the entire situation, bringing the case to a successful conclusion.

While surveillances usually do not follow this scenario, those who have conducted such operations will admit that participating in a productive surveillance can be a rewarding and, at times, an exhilarating experience. Second only to operating confidential sources, surveillance is the most frequently employed investigative technique in obtaining arrests, indictments, and convictions for the FBI.

Unlike operating informants, however, conducting a surveillance requires using the team concept. The considerable resources required for a surveillance draw personnel away from other

investigative functions, which can pose problems. Also, the potential exists for alerting the subject of the investigation to law enforcement's interest, which conceivably could compromise the covertness of not only the surveillance but the entire case. Preparation and some fine-tuning at the onset can make the difference between having a productive surveillance and expending expensive resources and coming up empty-handed.

Law enforcement agencies primarily use surveillance to develop both intelligence and evidence to further investigations by identifying subjects, their

activities, and their associates, along with their residences, places of business, hang-outs, and other related locations. Surveillance also can identify potential sources, corroborate source information, provide security to undercover operatives, and gather data for site surveys. In addition, information obtained from surveillance can provide the probable cause for obtaining authorisation for other investigative techniques, such as search warrants and wiretaps.

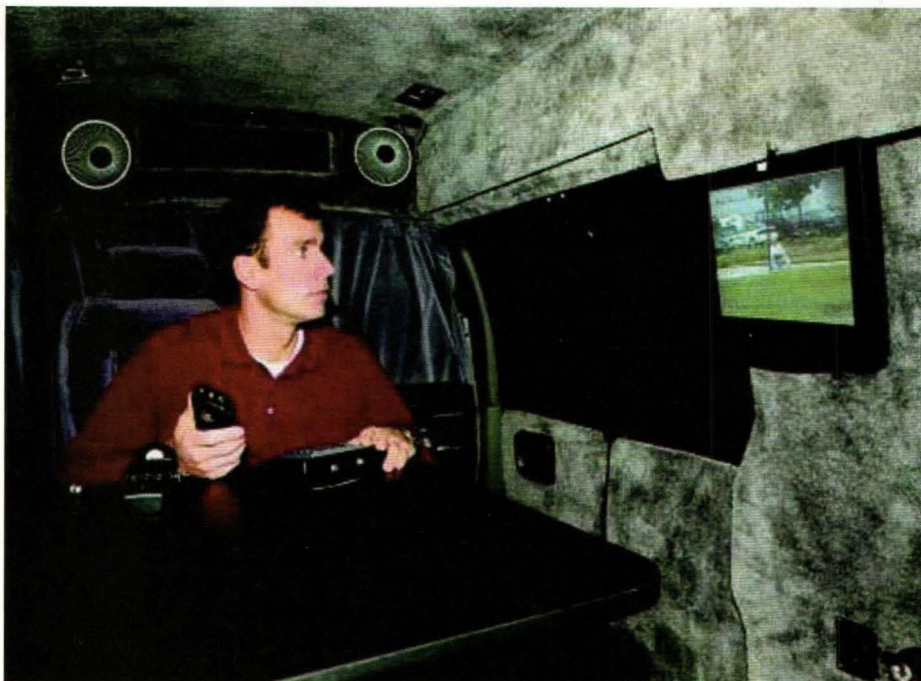
PLANNING AND PREPARATION

Once investigators decide that surveillance is appropriate, their agency's policy will determine what levels of authorisation are needed and how to allocate the necessary resources to the surveillance. Agencies should coordinate planned surveillances on a strict "need-to-know" basis.

At the onset, case managers, in conjunction with the physical surveillance, should consult technical services personnel to explore the feasibility of employing various measures, such as the use of video concealments, remote video, or tracking devices. Employing technical coverage or aircraft can function as force multipliers and enhance overall effectiveness, which can make the difference in obtaining productive results.

Prior to initiating the surveillance, investigators should update subject information to ensure that they have the most current available. For example, a motor vehicle or utility check and tail source contacts can save a lot of wasted time by revealing that the intended subject recently relocated or sold a vehicle. All team members should receive pertinent details, easily contained on a pre-printed form, to include:

- the case background;
- the surveillance objective;
- the subject's caution statement (e.g., armed and dangerous or known to possess a firearm);
- the subject's previous experience with surveillance and whether the subject appears surveillance conscious; and
- the subject's personal data (e.g., all descriptive data with photo; criminal history; habits, such as martial arts practitioner or bodybuilder, and associates; the vehicles of the subject and associates; and the locations of residences, work, and hang-outs).



SURVEILLANCE COMPONENTS

Realising that staffing constraints often become an issue in determining the amount of members available for a surveillance, a team of six generally proves optimal for a moving surveillance. Having a larger team reduces the chance of losing the subject and limits exposure of individual team members, enabling the surveillance to remain undetected.

AREA SETUP

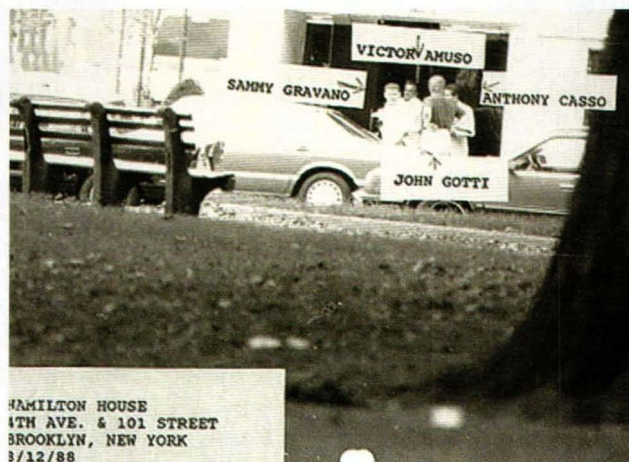
Prior to setting up at a location, surveillance team members should hold an operational briefing to disseminate last-minute updates and to conduct a roll call. Then, they should check their communications, including primary and alternate radio frequencies; review their procedures and assignments, ranging from team leader to log keeper; and inspect their equipment and vehicles, including topping off fuel levels of all vehicles. One

unit should conduct a site reconnaissance to assess the area in general and to specifically identify a location to set up the "eye" (i.e., the primary observation point) - or, if necessary, "eyes" - and to determine the likely routes of approach and departure, traffic patterns, and the location of bus stops and train stations, as well as areas to avoid, such as known criminal hang-outs.

Once the eye is in place with as unobstructed a view as possible of the subject location, the other team members should position themselves so they cover all potential departure routes. They should minimise driving by the location and congregating in the area as these practices can alert the subject or the subject's associates to a law enforcement presence. In addition, keeping the radio volume low and concealing law enforcement equipment in vehicles can help team members remain undetected.

FBI SURVEILLANCE PHOTO

Underboss Salvatore 'Sammy the Bull' Gravano notoriously testified against the infamous boss of the Gambino family, John 'Dapper Don' Gotti



Law Enforcement Picture Library

The specialist photo library for law enforcement and related images

Stock images for all your editorial requirements



Commissions undertaken for location and studio work domestic and foreign



Specialist models and props for advertising, promotional and illustrative requirements



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



The Law Enforcement Picture Library, P O Box 33699,
London, N16 6YT, UK
Tel: 020 8806 3037 Cell: 07951 054 092
Website: www.lepl.co.uk email: leplinfo@aol.com

MOBILE SURVEILLANCE

Once initial movement occurs, the eye calls out a description of the subject, always keeping radio transmissions as brief as possible. Because either surveillance detection or losses of the subject generally occur shortly after initial movement, team members should remain alert and exercise extreme care at this point. While time, distance, and conditions determine how long any team member stays with the subject, a rule of thumb is to maintain one or two vehicles between the team member and the subject and "hand off" the subject to another team member after taking one turn.

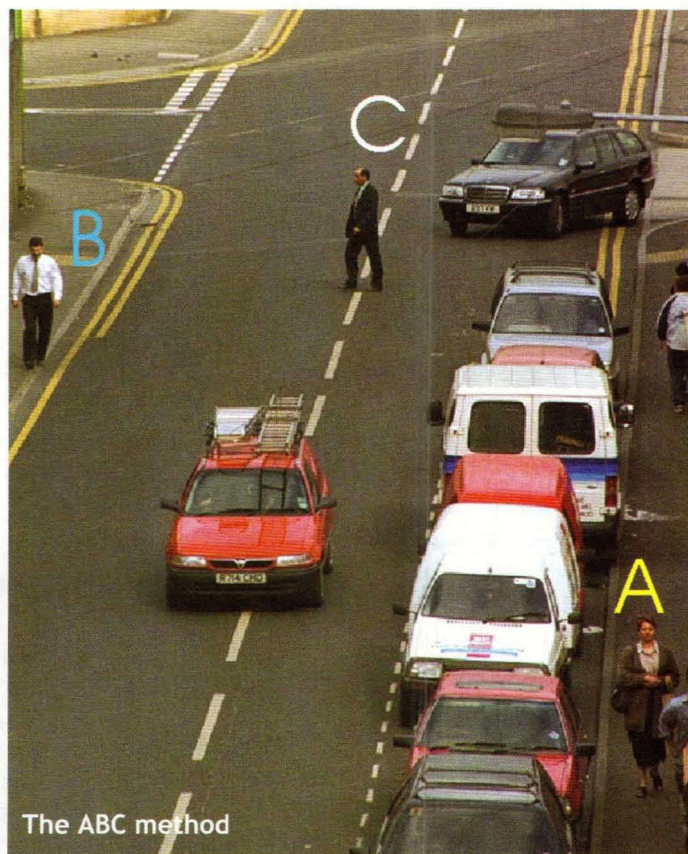
If the subject is on foot or uses public transportation, team members designated as "legs" should quickly exit and secure their vehicles to assume foot surveillance. On foot, the team adopts an ABC method, wherein the primary eye rotates between team members with at least one team member on the opposite side of the street from the subject.

STATIC SURVEILLANCE

In situations where the surveillance is static (i.e., immobile) or for mobile surveillances that become stationary, staffed vehicles parked on the street are effective for a limited time only. Once team members realise that a particular location will require surveillance for a protracted period, they should use speciality vehicles, such as vans or other utility vehicles, out-fitted with closed-circuit television or remote video.

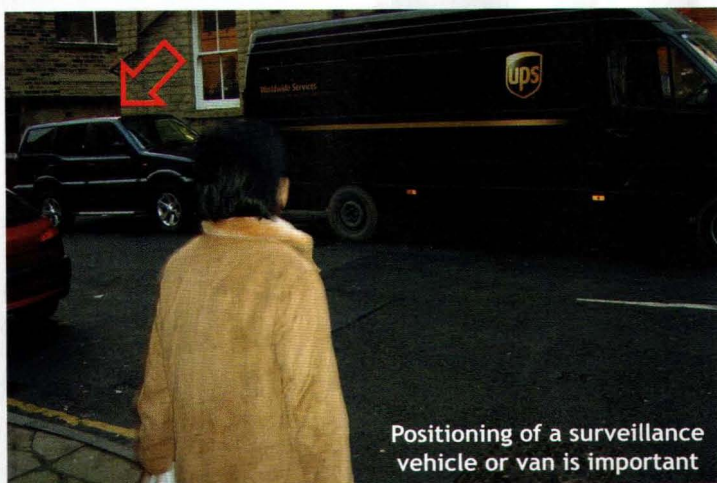
DOCUMENTATION AND LOGS

One team member maintains a chronological log to document observations made collectively by the team. Once completed, each team member initials each entry in the log, reporting



The ABC method

© PETER JENKINS ADVANCED SURVEILLANCE ISS



Positioning of a surveillance vehicle or van is important

observations they personally witnessed. The team leader reviews it for accuracy; afterwards, the agency retains the original in the official file as evidence. Investigative personnel receive copies in a timely manner for analysis and logical follow-up.

SURVEILLANCE PHOTOGRAPHY

In addition to the written logs, still photographs and video footage provide visual documentation of an occurrence and constitute the work product of a surveillance. The mere existence of photographs has resulted in countless jury convictions and guilty pleas being entered, thereby saving prosecutor's offices and law enforcement agencies months of trial preparation, as well as the trial itself. For this reason, investigators should attempt to obtain the highest quality surveillance photographs whenever possible.

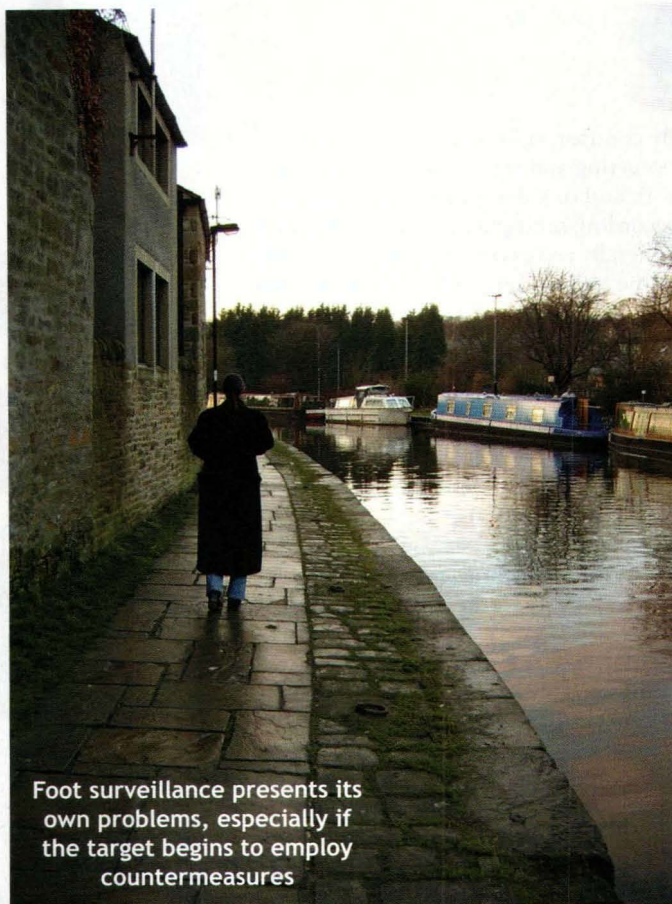
DIGITAL VERSUS CONVENTIONAL

The conversion from conventional to digital photography has not posed any significant evidentiary problems to date. While it is common knowledge that digital photography images can be easily

manipulated, this also holds true when using conventional photography. However, a variety of authentication methods can maintain the integrity of a photo. In addition, adherence to an established handling procedure, such as the use of write-once read-many (WORM) media, further reduces vulnerability from a legal challenge.

STILL VERSUS VIDEO

Which type of photos, still or video, is more desirable for surveillance purposes? If possible, investigators should obtain both because both have advantages and drawbacks.



Foot surveillance presents its own problems, especially if the target begins to employ countermeasures

The overall picture quality of still photos generally proves superior to video, even when obtaining a freeze-frame. Additionally, telephoto lenses needed in surveillance photography are more readily available for still cameras. And, individuals can view still photos more easily without the need for a monitor or VCR. A few rules can assist investigators in obtaining high-quality still photos (see below).



- Because most investigators are not professional photographers, they should familiarise themselves with the features of a camera before taking it on a surveillance.

- Prior to taking photos, they should clean the camera lens and

vehicle wind-screen.

- When taking photos from a vehicle, they should turn off the engine and film from a stabilised position using a tripod or make shift devices, such as the steering wheel or dash board with a towel or

beanbag for support.

- They should not delete any photos taken.

- When photographing from behind tinted glass, they should remember that they will lose at least one f-stop (i.e., the function that regulates the



amount of light coming through a camera lens).

- To prevent being revealed from back lighting, they should place a dark cloth behind them.

EYE SPY

SUBSCRIBE

INTELLIGENCE MAGAZINE



By contrast, video records the action occurring and can be used in conjunction with audio. Video cameras are capable of recording multiple frames per second and generally are easier to operate than some of the high-quality still cameras. To obtain quality footage when using video, investigators should:

- **set the video camera on manual focus;**
- **clean the lens and vehicle windscreen;**
- **video continuously, minimising camera movement and zooming;**
- **activate the date and time feature and ensure that the correct time and date are displayed;**
- **use the eye piece as the LCD can illuminate them, as well as rapidly expend battery life; and**
- **upon completion, label the tape as the original and include their initials, time, date, and case identifier, as well as slide or remove the write-protect tab to prevent accidental erasure and make copies, labelling them as such.**

SURVEILLANCE RISKS

Investigators should always assume that subjects engaged in operational, terrorist, or criminal activity will attempt to detect surveillance by employing a variety of methods and techniques. For example, as part of al-Qaida specialised training, operatives are instructed to follow meticulous operational security. Tactics include conducting dry runs prior to becoming operational, using secondary roads and public transportation to flush out surveillance, and employing prearranged signals to communicate the absence or presence of surveillance to other al-Qaida members.

Criminal subjects, particularly drug violators and organised crime figures, employ a variety of measures to detect surveillance, including the use of neighbourhood lookouts and tail cars. During surveillances, participants must remain vigilant and alert to the possibility of countersurveillance techniques being employed against them.

Of paramount importance, investigators must remember that many in their profession have been assaulted, injured, and even killed while performing surveil-

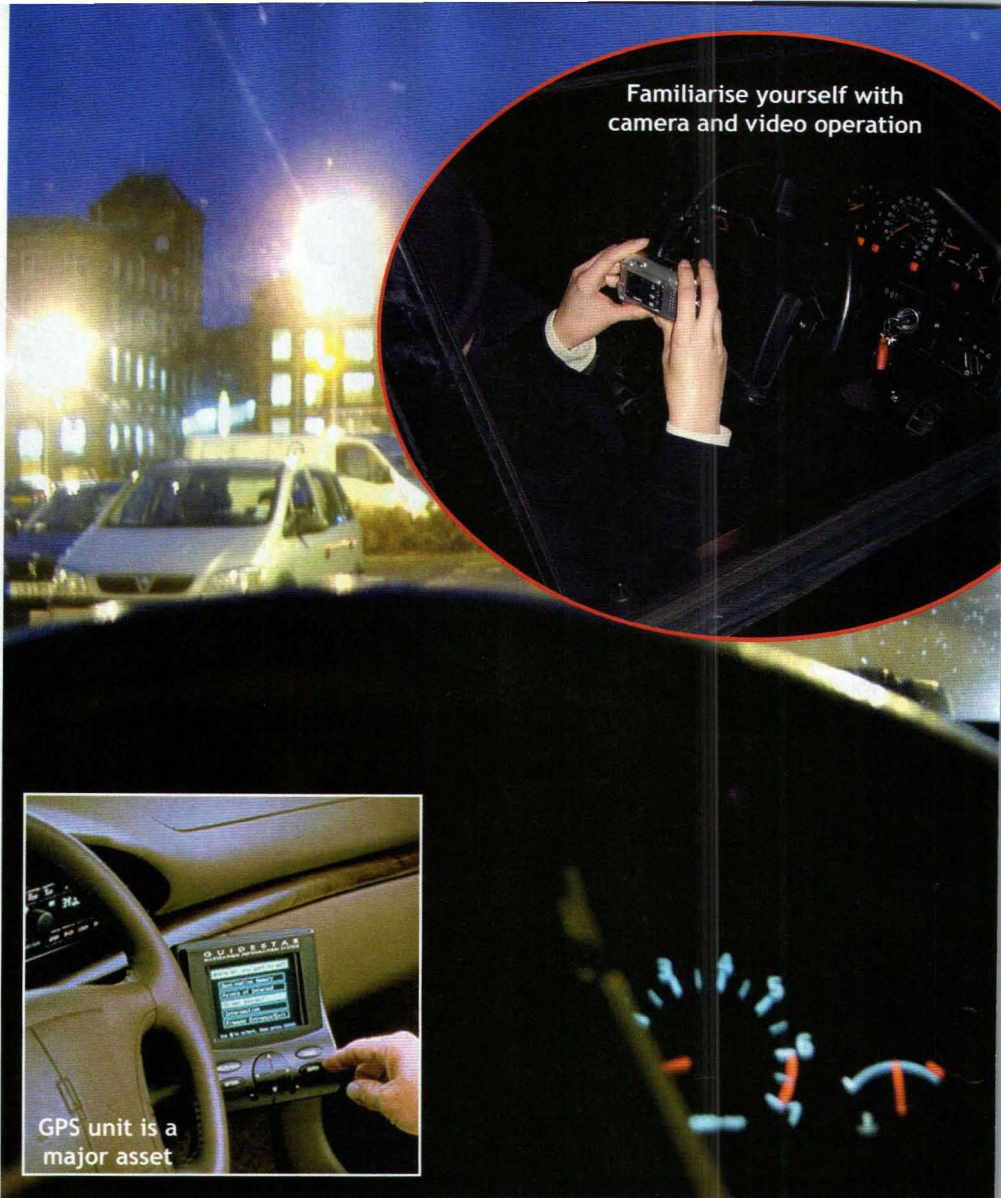
lance duties. For this reason, those involved in a surveillance must remain constantly aware of potential safety hazards. A dangerous situation can develop at any time, and investigators never should take it lightly. This becomes

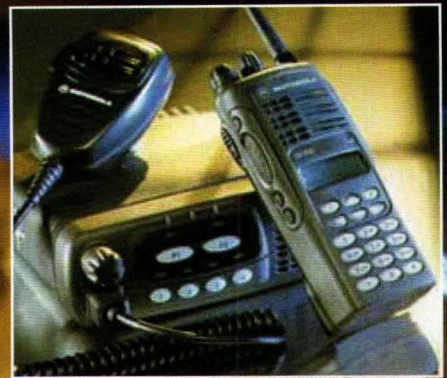
compounded when the surveillance occurs in a high-crime area and in hours of darkness. Risk assessments should be carried out at every level on an ongoing basis, which may result in the surveillance being terminated (see below).

SURVEILLANCE TERMINATION

Often, the decision to terminate a surveillance can prove as difficult as the one to initiate it. Investigators should consider the following factors when deciding whether or not to terminate the surveillance:

- **Assuming that the resources still exist, do the present circumstances warrant allocation of these considerable reserves at the expense of other cases or investigative functions?**
- **Is the surveillance still providing intelligence or evidence?**
- **Considering that the longer duration of the surveillance coverage increases the likelihood of detection, does the potential for gains outweigh the increased risk of detection?**
- **Would other investigative techniques or technical coverage prove more appropriate? After all, investigators always can always cut back or reinstitute the surveillance if needed.**





Two-way radios - essential

Investigators should always assume that subjects engaged in operational, terrorist, or criminal activity will attempt to detect surveillance by employing a variety of methods and techniques

Stay alert and focused at all times

SURVEILLANCE KIT CHECKLIST

- Department two-way radio ☒
- Hand-held portable radio with harness and fully charged spare battery ☒
- Mobile phone ☒
- Still camera with telephoto lens, adequate supply of film or other removable medium, and spare battery ☒
- Video camera with supply of tapes and extra battery ☒
- Stabilising device, such as a portable tripod ☒
- Binoculars and portable infrared or thermal-imaging devices ☒
- Detailed road maps for the area ☒
- Compass or Global Positioning System receiver ☒
- Flashlight with extra batteries ☒
- Change of clothing with props, such as hats, to alter appearance and other personal items, including toiletries ☒
- Food and water in a cooler ☒
- Cash, including coins to use at toll lanes requiring exact change, and toll passes ☒
- Extra set of car keys ☒
- Towels and glass cleaner ☒
- Equipment bag to hold above items ☒

CONCLUSION

Surveillance is a valuable investigative tool and like most other law enforcement endeavours careful planning can go a long way toward increasing the chance of success. Because surveillance is such a resource-intensive operation, it remains incumbent upon those overseeing such efforts to ensure the efficient and effective use of such limited resources.

A successful surveillance not only can bring a case together but can also prove

one of the most professionally and personally fulfilling experiences in a law enforcement officer's career. Moreover, it can help law enforcement professionals accomplish their sworn duty of preserving the peace and safeguarding the citizens of their communities.

© John T Nason/FBI

Editor's note: Eye Spy is extremely grateful to the FBI Bulletin for allowing publication of this feature.

SAFETY AND SECURITY MEASURES

- Alert other team members to any suspicious or unusual persons or activity in the area.
- In high-crime areas and in hours of darkness, remain in a heightened state of alert.
- Position vehicle to enable a rapid response to assist others if needed.
- Ensure vehicle has emergency equipment lights, siren, and first-aid kit.
- During a mobile surveillance, do not take unnecessary risks to keep up with a subject speeding, running red lights, or otherwise driving recklessly.
- While stationary, keep the vehicle windows closed and the doors locked.



- Regularly scan rear view mirrors to observe anyone or any activity to the rear.
- Keep identification, weapon, and ballistic vest assessable.
- Know and use challenge, pass-word, and other appropriate safety measures to prevent friendly fire situation from developing.
- When leaving a vehicle to go on foot surveillance, fully secure the vehicle and equipment inside.

THE GHOST

Wanted by Spanish intelligence, and a host of rather unsavoury characters, Señor Paesa died of a heart attack in Thailand in 1998. A few months later, Paesa's family posted an official death notice and invited religious figures to pray for him. The family duly received a death certificate. It was a bitter blow for the authorities who had scoured the planet for the rogue trader and spy, for he had been involved with money laundering to the tunes of several million pounds, much of it still unaccounted for.

Paesa was a leading agent in Spain's long and bitter intelligence war with the Basque separatist group ETA. During the mid-late 1980s, Paesa worked with the security services, and acted as a weapons broker who supplied missiles to the terror group. Unbeknown to those who received the goods, the missiles contained powerful transmitters and homing devices. Spanish intelligence soon arrested several key figures in ETA and managed to uncover a plethora of useful leads, overseas contacts and safe houses. ETA were none too pleased and suspected Paesa, but he remained one step ahead and continued to serve Madrid shadowy spy chiefs.

On another occasion, Paesa was central to a complex sting operation

that ultimately led to the arrest of Luis Roldán (right), a crook and former head of Spain's Civil Guard.

Roldán had been under surveillance for some time, but the security services needed to get close to him and his contacts in order to discover how he was able to obtain huge amounts of money, and then make it 'disappear'. Paesa told Roldán, who was suspected of misappropriating public funds, that officials were "on to him" and he would help him escape the country with his funds intact.

Roldán was himself a major player in the secret war with ETA. In 1996 the government of Felipe González had used senior police officers to recruit "mercenaries" to infiltrate ETA. With an escape plan prepared Paesa smuggled Roldán out of the country and switched his looted money to accounts across the world - ready for him to access. Unfortunately for Roldán, Paesa doubled-crossed him and provided Spanish police with details of his whereabouts. Roldán was jailed in 1999, and for his efforts, Paesa received a cheque for £1 million from the authorities.

Unfortunately, Paesa disappeared shortly after the sting operation, and



Spain's most infamous spy returns from the 'grave'

"...the security services needed to get close to him and his contacts in order to discover how he was able to obtain huge amounts of money, and then make it 'disappear'..."

with him went details of all the bank accounts containing Roldán's estimated \$5 million haul. By the time Roldán had provided some details, a large chunk of the money was still missing, and the authorities suspected Paesa.

It seems members of ETA and the Spanish Government were not the only people looking for Paesa, for immediately after his disappearance, an unidentified man hired British and Mexican detectives to search for him - apparently he had defrauded the mystery man out of a small fortune. The private investigators travelled to several countries before taking an interest in a man who called himself Francisco Pando. He was living with a much younger girl in Luxembourg and held an Argentine passport. The passport gave his age as 54, but the investigators suspected he was much older. It transpired that Pando was in fact Paesa, but before they could act, Paesa used all his cunning and escaped again.

When details of his death emerged in Bangkok, Spanish police officers suspected the spy was again covering his tracks - perhaps for a final time. However, before the authorities could act, journalists from Spain's Interiú traced Paesa to Paris. As the former spy sat drinking coffee, they confronted him. He explained that his death had been a "great misunderstanding," and that he had returned all Roldán's stolen cash. "There was a shoot-out in Bangkok in which three people died and they mistakenly thought that I had died. If you want, I can show you my scars!"

Interiú took several photographs to confirm the meeting, which didn't please Paesa, who also claimed that the Russian Mafia were now on his trail. "If you publish those photographs, you will sink me. I will have to shoot myself. My life has reached rock bottom."

Observers of the underworld believe Paesa will probably live another day... in another country.

EYE SPY

INTELLIGENCE MAGAZINE

SUBSCRIBE

*using the
world's most
informed
Intel sources*

UNITED KINGDOM, USA, EUROPE, ROW

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

UK £25.00 ☐

USA \$48.00 ☐

EUROPE/ROW £30.00 ☐

Name: _____ Address: _____

Post/Zip Code: _____ Country: _____

email: _____

Please make your cheque or money order payable to: 'EYE SPY PUBLISHING LTD' -
NOTE: WE ONLY ACCEPT UK, USA AND CANADIAN CHEQUES/POSTAL ORDERS

I enclose Cheque/Postal Order for: _____ / _____



For credit card payment by Visa, MasterCard, Switch

Credit Card No: _____

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

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

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



UK, EUROPE, ROW

Send your subscription to:

Eye Spy Publishing Ltd

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



UNITED STATES OF AMERICA, CANADA

Mail your subscription to:

Eye Spy International

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

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

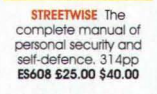
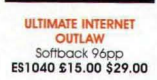


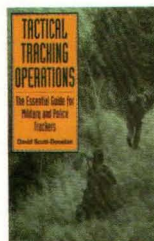
**TOLL FREE 7.00am - 4.00pm,
Mon-Fri 1-877-309-9243**

I N T E L L I G E N C E M A G A Z I N E

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

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

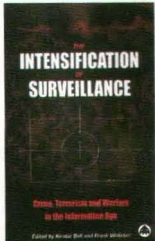




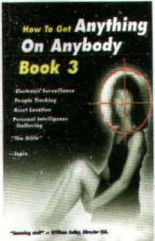
TACTICAL TRACKING OPERATIONS
The Essential Guide for Military and Police Trackers
Softback 170pp
£5827 \$38.00 \$60.00



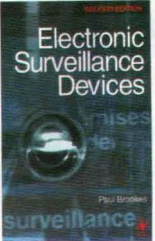
INVISIBLE ADVANTAGE
Grillie suit construction made simple. Softback 80pp
£5914 \$13.99 \$25.00



INTENSIFICATION SURVEILLANCE
Crime, terrorism and warfare. Softback 176pp
£5825 \$25.00 \$45.00



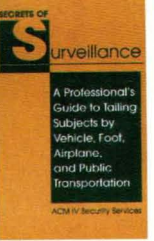
HOW TO GET ANYTHING ON ANYBODY
SPECIAL SECURITY WORK
Massive Softback
£5737 \$65.00 \$109.00



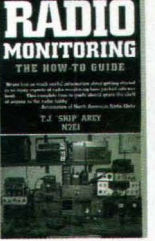
ELECTRONIC SURVEILLANCE DEVICES
Micro-phones, transmitters etc. 160pp
£5807 \$24.99 \$45.00



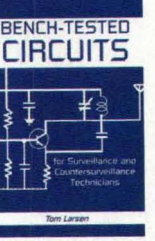
RECOGNISING BIO ATTACKS Anthrax, smallpox, nerve gas, radiation. Softback 112pp
£5870 \$17.00 \$23.50



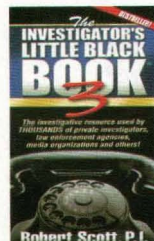
SECRETS OF SURVEILLANCE
Professional guide to tailing subjects. 248pp
£5814 \$29.99 \$50.00



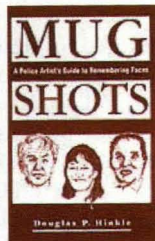
RADIO MONITORING
The 'know how guide' packed with tips. Softback 176pp
£5964 \$25.00 \$35.00



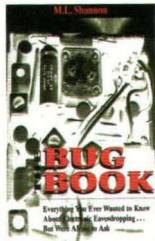
BENCH-TESTED CIRCUITS
For countersurveillance technicians. Softback 128pp
£5824 \$15.00 \$32.00



INVESTIGATOR'S LITTLE BLACK BOOK
Major US-based resource guide. Softback 504pp
£5806 \$19.99 \$35.00



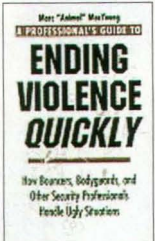
MUG SHOTS
A police detective guide to remembering faces. Softback 128pp
£5880 \$20.00 \$38.00



BUG BOOK Everything you wanted to know about electronic eavesdropping. Softback 168pp
£5907 \$30.50 \$50.00



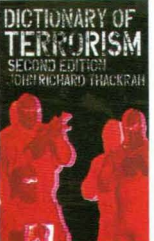
SPY GAME Winning through super technology. Huge Softback 520pp
£5862 \$35.00 \$60.00



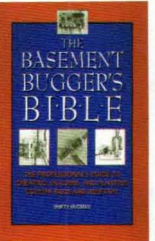
ENDING VIOLENCE QUICKLY Avoid injuries and law suits - professional guide. Softback 256pp
£5894 \$21.99 \$40.00



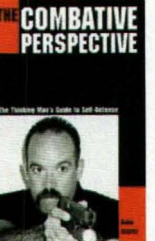
EXECUTIVE PROTECTION A professional's guide to bodyguarding. Softback 112pp
£5872 \$15.50 \$31.00



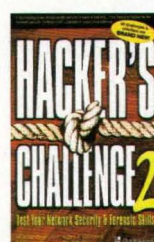
DICTIONARY OF TERRORISM Every group, individual listed. Essential. Softback 448pp
£5975 \$25.00 \$48.00



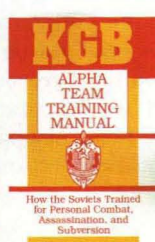
THE BASEMENT BUGGER'S BIBLE Everything you need to know about bugs. Softback 312pp
£5947 \$34.99 \$60.00



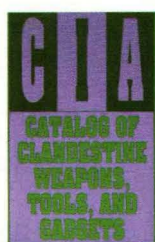
COMBAT PERSPECTIVES The thinking man's guide to self-defence. Softback 112pp
£5884 \$17.50 \$34.00



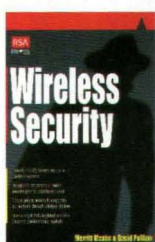
HACKER'S CHALLENGE 2 Test your security and forensic network skills. Large Softback 320pp
£5982 \$25.00 \$48.00



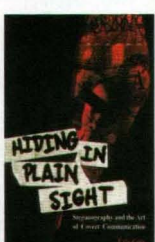
KGB ALPHA TEAM TRAINING MANUAL Combat, assassination and subversion. 320pp
£5808 \$24.99 \$45.00



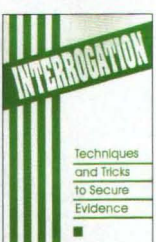
CIA CATALOG Clandestine weapons, tools and gadgets. Softback 128pp
£5944 \$18.00 \$28.00



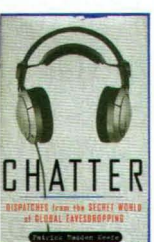
WIRELESS SECURITY Professional tips to secure your wireless network. Softback 300pp
£5980 \$25.00 \$49.99



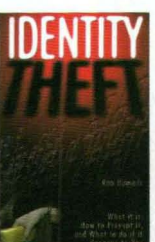
HIDING IN PLAIN SIGHT Super guide to steganography plus CD ROM. Softback 335pp
£5802 \$27.00 \$45.00



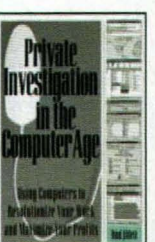
INTERROGATION RCMP guide. Techniques and tricks to secure evidence. Softback 88pp
£5811 \$19.50 \$38.00



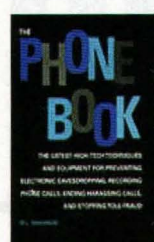
CHATTER Conversations from the secret world of eavesdropping. Hardback 300pp
£5950 \$25.00 \$35.00



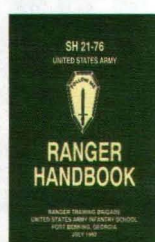
IDENTITY THEFT Secrets of counter identity theft and protecting yourself. Softback 241pp
£5950 \$12.99 \$25.00



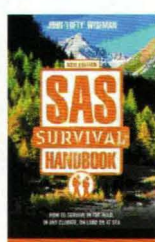
PRIVATE INVESTIGATION IN THE COMPUTER AGE Using computers. Softback 176pp
£5859 \$25.50 \$50.00



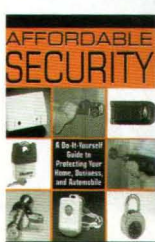
THE PHONE BOOK Stop eavesdroppers, telephone bugs, phone call fraud and more. Softback 280pp
£5858 \$30.00 \$60.00



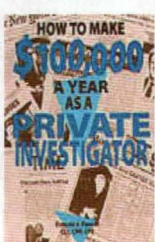
RANGER HANDBOOK US Army Ranger. Rare small manual. Softback 448pp
£5810 \$26.00 \$48.00



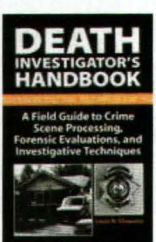
SAS SURVIVAL HANDBOOK Survive in any climate, land or sea. Softback 576pp
£5830 \$24.00 \$45.00



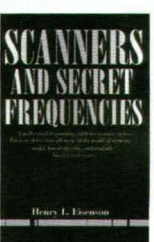
AFFORDABLE SECURITY Survive in any climate, land or sea. Huge Softback 302pp
£5830 \$24.00 \$45.00



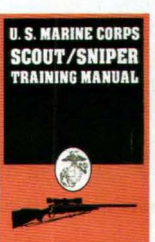
HOW TO MAKE \$100,000 A YEAR AS A PRIVATE INVESTIGATOR Field guide to crime scene forensics. Massive Hardback 888pp
£5879 \$75.00 \$100.00



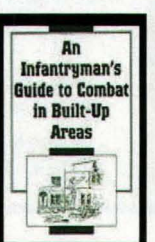
DEATH INVESTIGATORS HANDBOOK Field guide to crime scene forensics. Massive Hardback 888pp
£5879 \$75.00 \$100.00



SCANNERS AND SECRET FREQUENCIES All you need to know. Softback 314pp
£5967 \$25.00 \$38.00



SCOUT/SNIPER TRAINING MANUAL Product of US Marine Corps. Softback 576pp
£5959 \$29.99 \$40.00



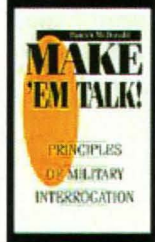
COMBAT IN URBAN AREAS Ground operations in urban settings. Softback 312pp
£5888 \$29.99 \$58.00



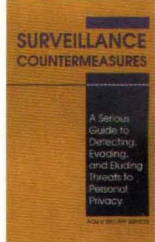
KILL OR GET KILLED Longest-selling book on close combat in history. Softback 420pp
£5889 \$45.99 \$80.00



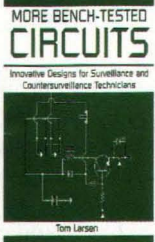
THE WHOLE SPY CATALOG Everything you need to know about espionage. Softback 448pp
£5886 \$35.00 \$55.00



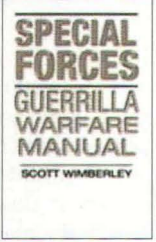
MAKE 'EM TALK Principles of military interrogation. Professional guide. Softback 80pp
£5890 \$17.99 \$35.00



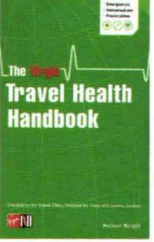
SURVEILLANCE COUNTERMEASURES Detecting, evading and eluding threats. 180pp
£5835 \$29.99 \$48.00



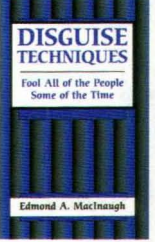
MORE BENCH-TESTED CIRCUITS Innovative designs for surveillance and countersurveillance techniques. Softback 72pp
£5909 \$19.99 \$38.00



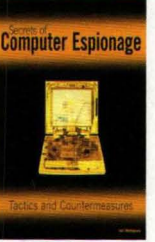
SPECIAL FORCES GUERRILLA WARFARE MANUAL Guerrilla warfare manual for successful operations. Softback 248pp
£5912 \$22.99 \$42.00



VIRGIN TRAVEL HEALTH HANDBOOK - 2003 Business, professional or casual travel. 288pp
£5727 \$17.50 \$34.00



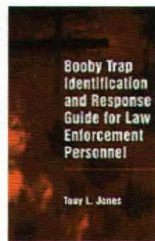
DISGUISE TECHNIQUES Fool all of the people some of the time. Softback 82pp
£5962 \$18.00 \$28.00



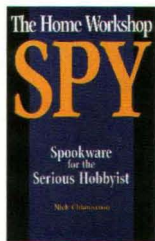
SECRETS OF COMPUTER ESPIONAGE Tactics and countermeasures. Softback
£5790 \$25.00 \$46.00



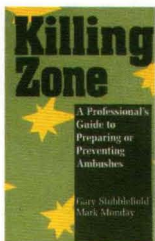
THE EXTREME COVERT CATALOG - SPECIAL TRADE SECURITY WORK - IMPORTED. Massive Softback
£5738 \$50.00 \$60.00



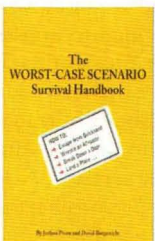
BOOBY TRAP IDENTIFICATION Response guide for law enforcement personnel. Softback 80pp
£5876 \$20.00 \$38.00



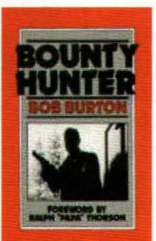
HOME WORKSHOP SPY Spookware for the serious hobbyist. Softback 104pp
£5856 \$24.50 \$48.00



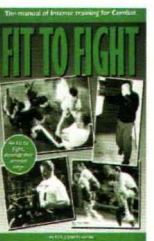
KILLING ZONE A professional's guide to preventing ambushes. Softback 240pp
£5960 \$25.00 \$40.00



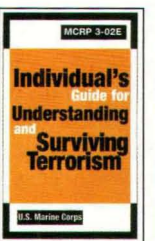
WORST-CASE SCENARIO TRAVEL Survival handbook. Softback 192pp
£5805 \$12.00 \$24.00



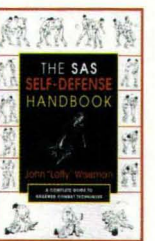
BOUNTY HUNTER Professional guide to the art of bounty hunting. Softback 136pp
£5873 \$15.50 \$30.00



FIT TO FIGHT Complete manual of intense training for combat. Softback 163pp
£5654 \$18.00 \$30.00



SURVIVING TERRORISM Packed with essential tips and advice. Softback 86pp
£5971 \$12.50 \$18.00



SAS SELF-DEFENCE HANDBOOK Complete guide to unarmed combat. Softback 240pp
£5831 \$29.99 \$48.00



the name of another man was also retrieved, however, Boutrab had placed his own picture in the photo section. He also went by the name of Fabio Parenti - an Italian - though it was quickly ascertained he had taken this identity from documents stolen from an Italian citizen at Dublin airport a couple of years earlier.

An intelligence-led raid on Boutrab's apartment followed. Police discovered over 20 floppy discs and dozens of audio tapes and several mobile phones. After forensic analysts started to check a variety of other items, they discovered CD-Roms containing weapons and explosives instructions that were far from passive. The material had been downloaded from the central library in Belfast about 12 weeks earlier by Boutrab who held a library card. A London Underground (Tube) ticket and several passport-sized photographs of Boutrab were also recovered. Boutrab was arrested and since spent the last two-and-a-half years on remand in Maghaberry Prison.

End of the 'Identi'

Aeroplane bomb plotte

Thirteen years ago an Algerian youngster known as Abbas Boutrab was arrested by French security officials in Paris. He was detained for stealing a handbag in the city. Since then he has traversed the world using a plethora of false identities and passports and has been linked to various crime gangs. Unbeknown to Boutrab various security services, including MI5 and the FBI kept him on record: but Boutrab was a skilled forger and using numerous identities soon disappeared into the underworld. He was also a "person of interest" in Holland, France and Ireland. Over the next few years Boutrab's mazy life of crime eventually led him to the arms of al-Qaida.

By early 2003, MI5 had received many intelligence warnings that al-Qaida were planning to crash or destroy an airliner over central London. Locations in England were monitored, but few officers believed a major clue would emerge in Northern Ireland, and in particular, on the Whiteabbey estate in north Belfast. British immigration officials raided an apartment in the area following a disturbance. They decided to question the occupier on the adjacent flat and were suspicious of the owner's identity. He said his name was Abbas Boutrab and was seeking asylum in the UK. After checking with the security services, Northern Ireland police officers suspected he was wanted by police in the Republic of Ireland under the name Yocel Djafari for attempted murder. A Dutch passport in



The instructions suggested that the bomb's components should be placed inside an object such as a personal tape recorder and reassembled inside the aircraft

An al-Qaida plan to attack London using aircraft has already been foiled by MI5. It is not known whether the UK's capital was the intended target in the case of Abbas



Two of the false passports used by Abbas



Man' jailed

The information on the computer discs was incredibly detailed and showed how to disassemble a bomb and smuggle it on board an aircraft inside everyday items. The intelligence was more than interesting, for MI6 and the CIA had already been forewarned that al-Qaida operatives had embarked upon such a programme. Two Russian airliners were destroyed by terrorists using such a ruse.

Besides the airline bomb data, officials also found information on how to construct a home-made silencer for an assault rifle using various materials readily available at do-it-yourself stores. Due to the nature of the discovery, MI5 was alerted and the downfall of Boutrab was inevitable. It was quickly discovered that Boutrab "had an allegiance to groups

associated with al-Qaida," an intelligence source said.

The improvised explosives' device 'manual' was sent to FBI specialists in America. One bomb-making official carefully followed the instructions enabling him to construct a bomb easily capable of downing an aircraft. On 14 December 2004 Dr Sachtleben, an explosives and hazardous devices examiner in the Explosives Unit of the Federal Bureau of Investigation received a copy of the instructions. Dr Sachtleben's conclusion was that the improvised explosive material was an extremely volatile mixture which when properly mixed and initiated could produce significant damage to the area immediately surrounding the blast. A person in close proximity to the explosion could be seriously injured or killed by the initial blast or any resulting fire. It was his opinion that the initiation of the device on an aircraft would be likely to result in damage to the aircraft and injury and/or death to passengers on board. It was stated to be his experience that explosions in a fully pressurised aircraft flying at cruising altitude was more likely to cause catastrophic failure than a similar explosion in an aircraft flying at low altitude or against a section of aircraft

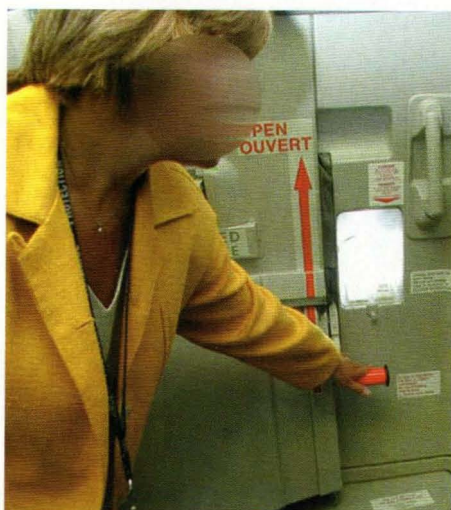
A Deadly Device

Aviation specialists have sufficient data to test the impact of explosives inside airliners. For example, in 1996, the FAA's Aviation Security Research and Development Division and the United Kingdom's Civil Aviation Authority collaborated to study blast effects on commercial wide-body aircraft and potential mitigation methods by exploding a pressurised Boeing 747-100 at Bruntingthorpe Airfield, Leicestershire, England (see photo).

In 2005, FBI bomb specialists reconstructed the device from data downloaded by Abbas Boutrab and confirmed it would have resulted in the catastrophic failure of an airliner.



END OF THE IDENTITY MAN



Aviation security officials regard the toilet area of aeroplanes as particularly vulnerable in respect that a bomb can be assembled out of sight from cabin crew

fuselage. Robert R Keller, a senior forensic examiner at the Audio, Video and Image Analysis Unit of the Operational Technology Division of the FBI, videotaped the explosives tests in Virginia. The same official travelled to Belfast and showed

the results of his investigation - conducted at the Quantico Marine Corps base in Virginia - a specialist site whose employees are at the forefront in devising methods to counter such devices. The video showed the assembled bomb inside a mock-up area of the passenger compartment. Once detonated, the blast destroyed seats and, more frighteningly, the skin of the aircraft.

Esmond Adair (below right), the lead investigator in the case said: "I believe he is an unrepentant terrorist." Judge Weatherup agreed: "Now we find the [Northern Ireland] terrorism threat is subsiding and a new threat is emerging. This new threat has an added horror because the terrorist stands amongst the innocent men, women and children. That's a feature in the material that was recovered..." [SIC] Judge Weatherup once again identified the emerging menace of IEDs. "The information provides instructions for improvised



explosive devices with the objective of bringing down an aircraft and the lives of all those on board." Mr Adair also said: "It is worthwhile remembering that those who are involved in this kind of terrorism are extremists and in no way representative of the vast majority of the law-abiding Muslim community."

For the intelligence services the arrest and jailing of Boutrab was a success, however, the real bonus comes in the fact that a likely terrorist operation was foiled, and the material seized in Belfast will undoubtedly lead to a worldwide search for his associates.

• Boutrab was tried under the UK's Diplock system, where a judge in a terrorist case sits without a jury. Mr Adair believes Abbas Boutrab was not his real name, but yet another assumed identity.



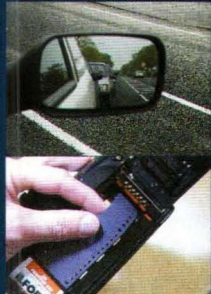
Abbas Boutrab



THE WORLD'S LEADING SURVEILLANCE TRAINING COURSES

**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




ISS TRAINING LIMITED Est. 1990




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



Presidents' Day Weekend
February 17-20, 2006

www.intelligencesummit.org

The international Intelligence Summit, intended to be the most prestigious world conference on intelligence policy and homeland security, is bringing together international intelligence agencies, top CEO's, Congressional leaders, and cutting-edge technology experts to share ideas in the common war against terrorism.

Hyatt Regency Crystal City Hotel
Arlington, VA

(Across the river from the Capitol, between
the Pentagon and Reagan National Airport)

HOSTILE ENVIRONMENT SURVIVAL

Security personnel, bodyguards, aid workers, the media and civilians working in conflict zones should be trained to deal with a multitude of dangers and situations that can arise when operating in foreign lands. Unfortunately this is not always the case. Many people venturing to such places are ill-informed and not prepared. Eye Spy looks at several key factors that should be addressed before selecting a place of residence.

A security guard was killed by an angry mob because he answered a question in the wrong language in the wrong part of town. An international relief worker was beaten to death for trying to help people on the wrong side of an island. There are many conflict zones outside the Middle East including the Balkans, Kosovo, Bosnia, the Congo, Sierra Leone, East and West Timor, Haiti, Colombia and since the 2001 attacks on America - almost any region can become a conflict zone. Environment training for working in foreign countries or disaster areas can be a matter of life and death.

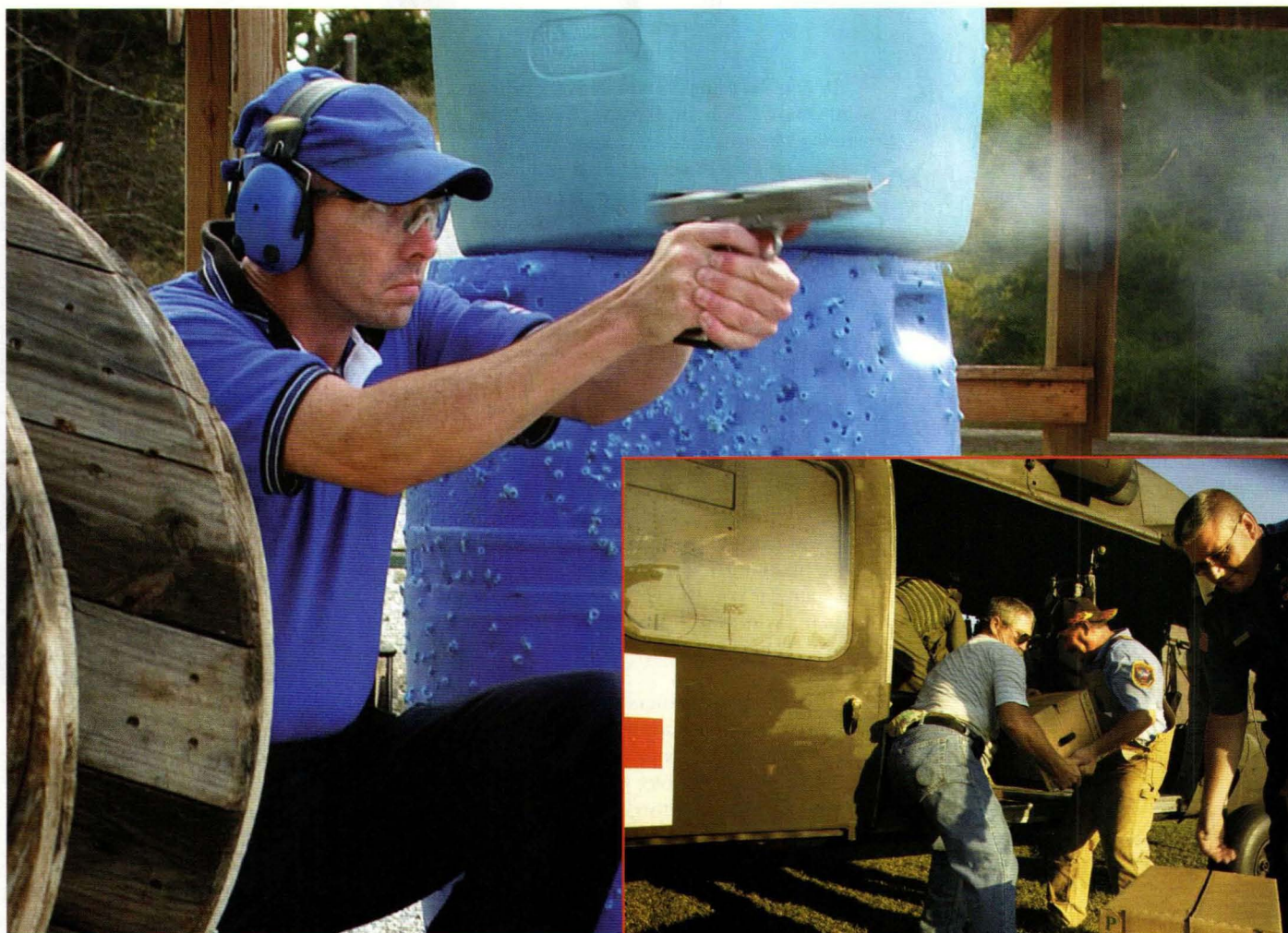
All too often we hear about persons being abducted in Iraq - and not necessarily just those assigned to security companies or government offices. For reasons right or wrong, everyone is vulnerable. However, there are many safeguards readily available that could lessen the risk. Naivety is no excuse when journeying into 'high intensity areas'.

RESEARCH BEFORE YOU GO

Proper research is essential. Read and absorb everything you can get your hands on about the area. Despite its obvious frailties, the Internet is a great source of information from both official and unofficial sites by people who live in the area. Although it may be propaganda, you'll get a reasonable idea of



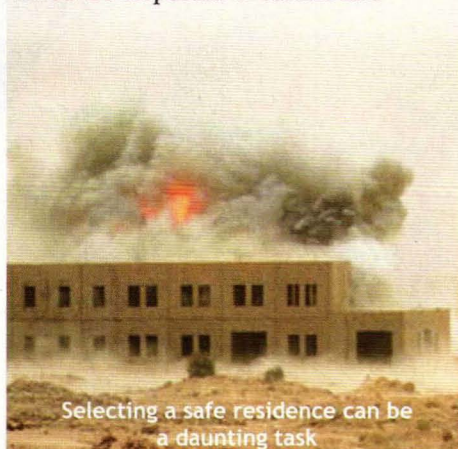
TRADECRAFT



Having a source of clean water is equally as important as having access to a firearm - in some cases it is far more essential

who hates whom and why. Research the history behind the hatred and politics and familiarise yourself with the ethnic groups and governments involved. Government web sites offer excellent advice on the status of most nations.

Learn what slogans, languages and clothing *not* to use and wear. When on-site, talk to locals and follow their advice - discover the meaning of colours in the region; in some countries even wearing the wrong coloured shirt can get you killed. Be respectful of culture and

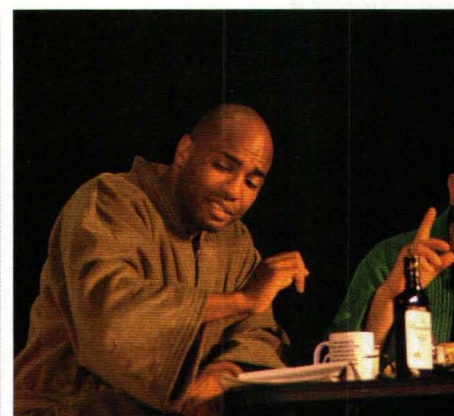


Selecting a safe residence can be a daunting task

traditions, but be aware at all times you are an invited guest or there to be of assistance. Just because you view your role as "helpful", doesn't necessarily mean everyone will.

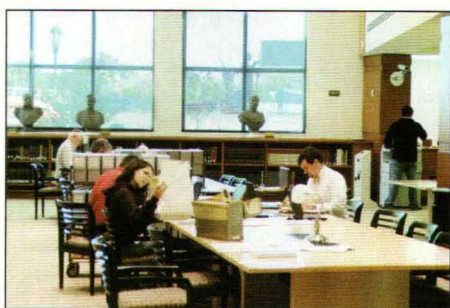
PASTEURISED

It's a harsh reality, but avoid eating local meat at all costs. With water and electricity often scarce or infrequent, meat can't be kept long and can make you extremely ill. Even if food is cooked correctly, it will take a while for your stomach to get used to the new bacteria. Be watchful about eating cheese or milk products and eggs. Sugar, rice and salt are often stored in open sacks and are frequently infested with unpleasant critters. And vegetables are no safe bet - proper fertilizer is hard to find so local farmers often rely on 'natural' fertilizer from the outhouse. Water can be even more dangerous. Water supplies can be dumping grounds for garbage and occasionally dead bodies. Don't drink the water unless you boil it 10-15 minutes or treat it with purification tablets. Just because locals drink it, doesn't mean it is safe. Make sure everything you eat or drink is pasteurized.



A nearby military base may allow you to use its canteen

Foreign nationals operating abroad should be able to provide details of recognised and safe restaurants. If your country has a military base nearby, see if you can be allowed to eat on the base or purchase goods from the base shop. If you are that fortunate, be polite and follow the rules. Drive the speed limit, let soldiers step in front of you in line; don't ever take more than you need. It can take only one infraction to get you banned from the base. ➤



Changing your travelling routine to and from work is advantageous

BE PREPARED

Do your homework - don't isolate yourself; try to stay near international workers. Find a place to live near a shopping area, spend as little time as possible on hazardous roads or conflict areas. When driving or walking to a regular place of work, change your route and time of travel as often as possible. Don't wear bright clothing or accessories that make you stand out.

Living near police or military checkpoints can be noisy and targets for snipers and bombers. Avoid living at the top of hills. Roads in poor conditions, especially in winter seasons can become inaccessible in snow. Spend a little time monitoring such features as buildings, shops and roads. This should provide a little useful background as to the standard of living and how well the area is maintained.

Familiarise yourself with locations that you may need in the event of any emergency, such as the nearest hospital or doctor. Again, it may be possible for you to utilise military base facilities.

In conflict zones, prospective landlords may move their families out in order to rent to international workers. Take your time and look at several places before making a choice. Don't be afraid to ask for more details and check to make sure everything is included. Don't sign contracts and make sure you can change the locks. If you use a vehicle, spend a little time everyday on routine checks to make sure that it has not been tampered with.

In some conflict areas electricity was a rare treat even before the bombs fell. A reliable compact flashlight is essential. Standard flashlights for your residence should be stored in easily accessible places. Acquire candles, matches, lighters, gas, oil lanterns and single-burner stoves - as many as you can get. Don't forget to open a window - it's better to be cold than asphyxiated.

Buy plastic containers to store water. Once you have a supply use it quickly and avoid wasting it. Water will stagnate after a few days. If possible, purchase a solar shower - but don't forget the funnel.

YOUR RESIDENCE

Overseas security personnel situated away from military compounds need to take great care before choosing a residence. Take a few minutes to walk around the property. Check for trees, posts or anything that could allow access to your windows. Don't choose a residence with doors or openings hidden from view. Windows that can be opened from the outside or latches on doors that are in poor condition pose serious problems.



Check the residence during day and night-time. This will provide useful information and give you some idea of the type of environment. Familiarise yourself with escape routes and the interior of the building. If you feel changes are necessary to the building, don't be frightened to ask the property owner. If he refuses, barter with him on a reduction in rent and use the extra money to complete the tasks. In most cases, the landlord will assist - losing a



Welding a metal plate behind a door may be a laborious task, but it could be a life-saver





A residence too close to a military checkpoint could expose you to dangers - including sniper fire or roadside bombs



Building a strong box, safe or even a secret hideaway could be beneficial

tenant will not be a palatable option for him.

The front door is important. Assess just how quickly you could gain entry. A door brace or wedge can provide valuable seconds if the door is being forced or attacked. If appropriate, a sheet of metal could be fixed on the door's interior to provide additional security. Check the frame of the door for damage or wear and tear. Position interior locks in the appropriate place on the door. This should foil most attacks, or at the very least give you

more time to prepare your next move. Windows accessible from the ground should also be examined and the necessary action taken to secure them. If the door is weak ask the landlord to replace it with solid wood or metal. If none of these are fitted, it is advisable to make other living arrangements until the property is properly secure.

Many attacks on such locations are random and 'hit and run'. Grenade-proof any window facing a street, alley or sidewalk. Simply tack chicken wire over the window or nail it to the frame suspended three inches from the glass. The grenade will bounce off and hopefully explode after the bounce. However, do remember that as well as stopping an attack on your residence, the meshing will almost certainly hinder your escape.

Entry points into the residence should be illuminated. Don't rely on local electricity and never try to do wiring yourself. Always carry a portable flashlight on a utility belt or key-ring.

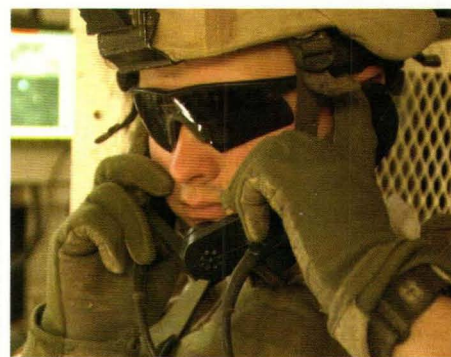
Poorly maintained wiring, dangerous heaters, fossil-burning stoves and arson

make fire the number one danger in a conflict zone. Make sure you install smoke detectors, a CO2 detector and have a good stock of batteries. In case of fire, study your exit options, or use a pre-determined escape plan.

If you can find a safe buy it. Find

one that can be bolted to the floor and big enough for all your valuables, documents and firearms. If possible, secret it

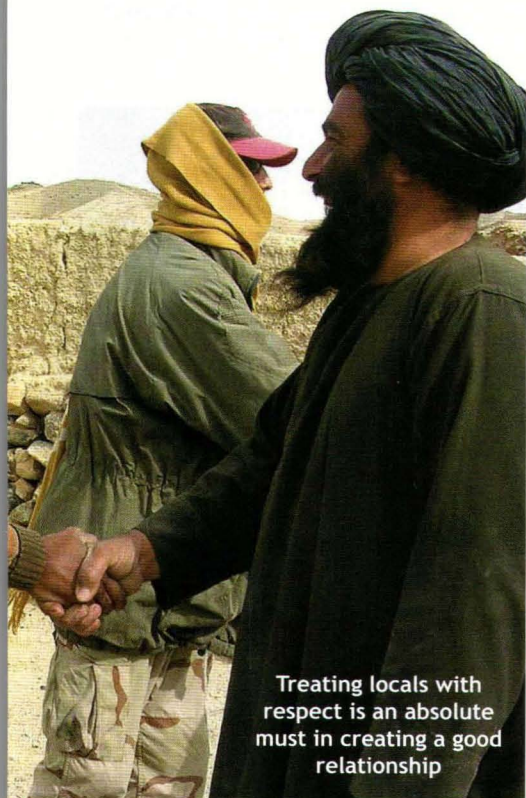
into the property and don't buy it in the town or area of residence. Even an innocent remark by the shopkeeper could be overheard by adversaries - or at the very least, criminals. Remember, a safe is an indicator that you have something to hide. Obviously such items are not always readily available, so it is worth spending a little time building a strong box or purchasing a metal case and improvising. If these options are unsuitable or impractical, find a suitable hiding spot in your residence. An excellent handbook providing dozens of concealment tips is *How to Hide Anything* (available from Eye Spy). Since it is highly unlikely you will have access to a safe bank, make sure you have some means to receive monies by wire transfer. When journeying on operations, carry only small amounts - sufficient for your duties for two or three days. ➤



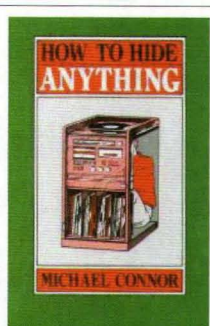
Communication tools are important



Finance during any stay in crisis areas must be handled differently



Treating locals with respect is an absolute must in creating a good relationship



How To Hide Anything - available from Eye Spy

Ref: ES/1117
£16.00 \$26.00



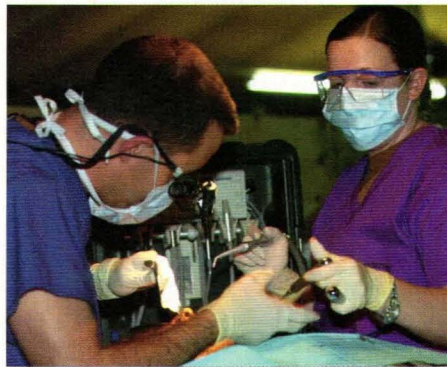
Fire is one of the biggest dangers faced by persons using unknown residences abroad in conflict zones

The remaining cash should be hidden in more than one location. This will lessen the impact if the cash is discovered by thieves. Regardless of where you hide the cash, always place bank notes in a plastic bag, this will help keep the money dry and in reasonable condition.

ESCAPE!

Many abductions in Iraq and other conflict areas take place in and around the residence. It is folly to rely on the local authorities to help in an emergency situation. However, by following the tips suggested in this Tradecraft feature, the very least you should be granted is valuable seconds to make good your escape. Once you have secured your residence, it is absolutely vital that you plan an escape route. However, it is just as important to make plans once you have

departed the location. Many security and aid firms refuse to allow workers to live by themselves. There is always safety in numbers. Similarly, such workers live in compounds or areas within walking distance of their work. Invite colleagues



Familiarise yourself with locations of the nearest hospital or doctor

to discuss security and create codewords that can be used to signal various alerts. Radios and communication are the lifeblood of many people working in conflict areas, keeping them in good working condition is paramount. Similarly, don't rely on just one device for communication - always have a backup plan.

Experienced security officers will spend time examining a residence and immediate area for escape purposes. Some properties may have adjoining lofts or basements that could afford immediate exits. By carefully loosening roof tiles and placing steps underneath, an escape via this route could be carried out in seconds. If your residence is impossible to customise or no escape routes are available, spend time creating a false panel that might double as a hiding place. Abductors rarely spend hours meticulously searching a residence.

HOME DEFENCE

If you don't know how to use a weapon don't buy one. Only keep a gun if you are authorised to have one, otherwise you'll get a visit from either the police or criminals wanting to steal it. A folding concealable knife is a good choice; don't use pepper spray in the house unless it is foam. A Kubaton can be kept handy and a flashlight (which you should always have with you) can double as a weapon.

Part Two follows in issue 39: Personal Safety Awareness, Basics of Self Defence, Items as Weapons, Capture, Escape and Evasion, Terrorist weapons

MI6 AND THE MACHINERY OF SPYING

By Philip H J Davies

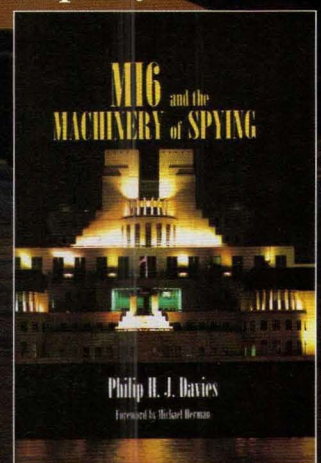
A key to unlock the door that holds the secret history and present day capabilities of the world's most famous intelligence service

Innovative research and analysis of the best kind: the study of intelligence organizations will never be quite the same again

Eye Spy Intelligence Magazine

Michael Herman

Available from Eye Spy Ref: ES/1056 £23.99 \$48.00





AGENT PARLOUR MAID

FBI Spy Case Collapses

The US Government dropped a complex spy case against Katrina Leung, 51, who was initially accused of working for Chinese intelligence as a double agent. The court accepted her guilty pleas of lesser charges - making false statements and irregularities with her tax return. Leung, an ex-FBI informant also acknowledged she had lied about an affair with her FBI handler, (now retired) 61-year-old James J. Smith. Approving a plea bargain between the prosecution and defence lawyers, Judge Florence Marie Cooper sentenced Katrina Leung to three years

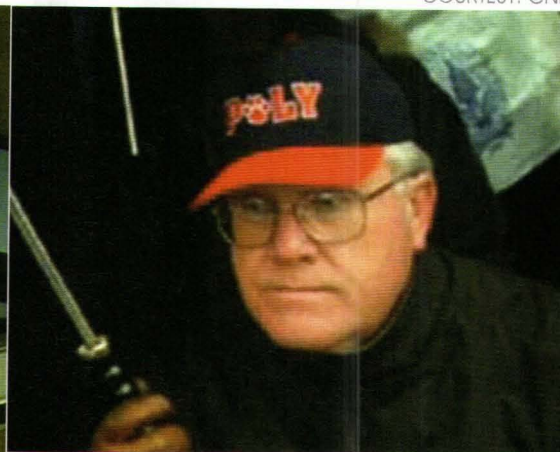
probation and fined her \$10,000. The espionage charges were dropped.

Leung was originally accused of illegally copying and possessing national security documents that she reportedly stole from her FBI handler and lover, FBI counterintelligence officer James J. Smith. Both Smith and Leung were arrested on 9 April 2003. At the time, Kam Leung, Katrina's husband, said: "This is blatantly unfair. For over 20 years, my wife had worked directly under the strict supervision of the FBI and, at the first sign of the two supervisors' sexual improprieties, the government immediately blew her cover, ruined her reputation and threw

her in jail, while the two male supervisors are either free or out on bail."

In January 2005, Judge Cooper ruled that the prosecution team had acted "unethically" by "exact[ing] a commitment from Smith" that in effect meant he could not be part of Leung's defence team. Prosecutors are not allowed to obstruct a criminal defendant's access to witnesses.

Described as a "socialite and business consultant" Leung travelled frequently to China and regularly mixed with senior diplomatic officials in Beijing and the USA. She also had access to former President Jiang Zemin, former



Former FBI counterintelligence officer James Smith

Premier Zhu Rongji and the late President Yang Shangkun, officials said. The FBI admitted that some of the information she forwarded was "first rate", according to documents filed in the trial.

Her handler, James Smith was a 30-year FBI veteran and an experienced counterintelligence officer. He headed the FBI's China division in Los Angeles. He recruited Leung as an informant/agent in 1983, but unbeknown to many of his colleagues, he also began a sexual relationship with her about that time. Smith retired in 2000. The FBI initially charged Smith with gross negligence in respect of handling classified documents. Like Leung, he also pleaded guilty to lying about their relationship - the couple said they were "just good friends." In 2005, he was given three months of home detention.

AIRBORNE SPY GAMES

Bugging the President's Aeroplane

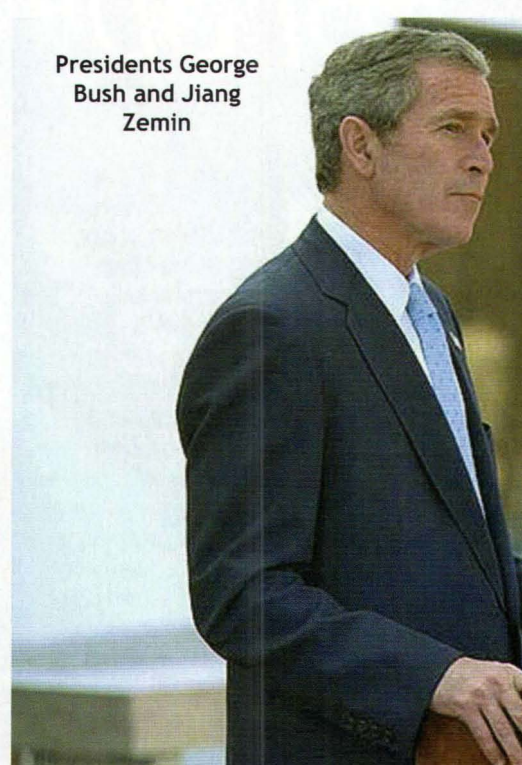
The United States and China have become bitter adversaries in the 'spying game', with China undoubtedly holding the upper hand. The FBI and CIA are wary of some 'legitimate' Chinese corporations and firms operating on US soil. There is little doubt some operations are simply front companies for China's huge intelligence network. However, it's not all one-way traffic if the Chinese are to be believed.

In October 2001, just days before its maiden voyage, Chinese intelligence officials discovered about 30 highly advanced listening devices planted inside a Boeing 767-300ER which was intended to act as President Jiang Zemin's official plane. The devices were reportedly activated by satellite and extremely small.

Chinese officials immediately blamed US intelligence agencies, and said undercover experts had planted the bugs aboard the plane while it was being refitted in the United States. One bug was found in a bathroom, and another carefully concealed in the presidential bedroom.



Presidents George Bush and Jiang Zemin



The case against Leung began when a number of FBI documents were discovered by investigators following a search of her home in San

Marino. The bureau had apparently been tipped-off by another FBI agent, William Cleveland, who also had an affair with Leung. Cleveland resigned as director of security for Lawrence Livermore Laboratory, a post he had taken after leaving the FBI. Smith was charged with gross negligence for allowing Leung to get hold of the papers. The FBI believed the material could harm US national security. One file contained personal details of FBI investigators involved in another Chinese spy case involving physicist Peter Lee. He had already pleaded guilty to passing classified information to Chinese scientists. A second file contained seven Xerox documents from the FBI's legal unit in Hong Kong which discussed Chinese intelligence gathering. The third file was an exact transcript of telephone calls and notes made between Leung and her alleged handler

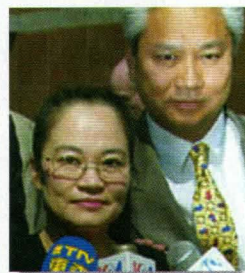


Former FBI counter-intelligence officer William Cleveland

at the Chinese Ministry of State Security in 1990 and 1991. Leung noted an FBI's forthcoming visit to China, and passed on information about a visit to the USA by relatives of a Chinese defector. With such material at hand, the FBI was convinced Leung was a double agent. Other conversations were also recorded using FBI wiretaps.

In 1991 Smith was confronted with the FBI material. After a further meeting in Washington DC, Smith was asked to "confront" Leung and prompt her to discuss what action to take. She told her lover that she "acted under duress" after Chinese counter-intelligence officers had "unmasked" her. It was apparently enough for Smith and the FBI - for he continued to use her as an informant - and the FBI appeared comfortable. It was not until 2002, the FBI looked into the matter again and internal affairs was asked to investigate their relationship.

When details of the spy case were revealed in 2003, then FBI Director Robert S. Mueller III decided to reorganise the service's counterintelligence section. Efforts were made to access the damage done in



Katrina Leung

respect of spy operations against the Chinese. A few months later China took delivery of a new presidential aeroplane from the USA. Within weeks Chinese intelligence officials had discovered some 30 eavesdropping devices carefully inserted in the aircraft's interior (see feature below). Other listening devices were also allegedly recovered in official Chinese diplomatic buildings in the United States. Suspicion immediately fell upon Leung that she had tipped-off Beijing. No evidence was found linking Leung to China's success in discovering the bugs.

Leung was paid a total of \$1.7 million by the FBI for her information as an intelligence asset code-named the 'Parlour Maid'.

LINKS: <http://www.pbs.org/wgbh/pages/frontline/shows/spy/leung/>



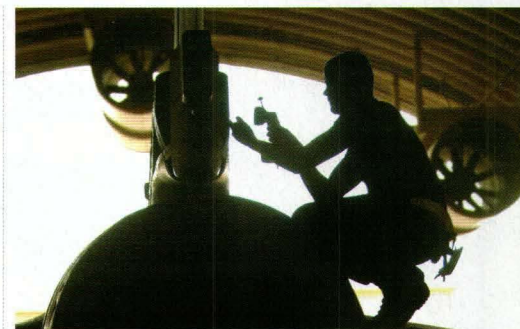
COURTESY: THE WHITE HOUSE

A Chinese source, with close ties to China's military intelligence services, said members of the Third Department of the General Staff Department of the People's Liberation Army discovered the devices. The Third Department deals in signals intelligence.

The Boeing was originally purchased by Delta Air Lines in June 2000, and later re-sold to China United Airlines - a Chinese air force operated run airline - and customized for executive use by Jiang by a modification company in Texas.

Unfortunately the incident occurred just five months prior to a planned summit between President Bush and Jiang in Beijing.

At the time, CIA officials quietly advised Beijing officials to look closer to home to find the culprits. Indeed, intelligence sources in Hong Kong said the Chinese



army may themselves have planted the surveillance devices. Twenty Chinese air force officers were questioned on suspicion of negligence and corruption, and two officials from the China Aviation Supplies Export and Import Corporation are in Chinese custody.

As for 'China United Airlines', it is well known to be a semi-front company for the military and at least one airliner is equipped with an array of spy technology.

Intelligence Fail



Hercules downed shortly after Black Hawks came under attack

An RAF Hercules C130 that crashed shortly after taking off from Baghdad International Airport last January, was shot down by insurgents. However, an official board of inquiry said that better intelligence and communication between UK and US forces may have prevented the incident. All ten men on board the aircraft died after it was struck by persistent small arms fire and rocket-propelled grenades. British intelligence believe the overflight area had been specifically chosen by al-Qaida or insurgents due to low-level aircraft or helicopter traffic.

After selecting the route of the 40 mile journey from Baghdad to Balad air base, the crew of XV179 set off at just before 16.22GMT on 30 January. Six minutes later the aircraft was in trouble. The crew radioed: "No duff [reference to a real occurrence], no duff... we are on fire... we are on fire." US Special Forces rushed to the scene and discovered the wreckage about 25 minutes after the crew's final message was received. An al-Qaida video that showed wreckage of the aircraft was aired a few hours later on Arabic television.



ire?

"...there is a need to ensure that compartmentalisation of information does not lead to elements of the force operating in ignorance of vital information..."

The report said: "The board has determined that the aircraft crashed as a result of hostile ground-to-air fire which caused an explosion in the right hand wing fuel tank."

"This explosion caused the outboard section of the wing to separate from the rest of the wing at which point the aircraft immediately became uncontrollable."

What is now known, is that a few hours before the Hercules was shot



Black Hawk Helicopter



COURTESY: US ARMY

down, two US Black Hawk helicopters travelling over the same area came under attack. The board of inquiry report stated: "The intelligence suggests that insurgents had prepared an ambush site." Air Chief Marshal Jock Stirrup, the Chief of the Air Force Staff, noted that the US intelligence on that attack was compartmentalised for security purposes. He also said that at the time there was no system in place where Coalition forces could share such intelligence.

Critics say that the intelligence should have been passed on to the crew of XV179, but Sir Jock refused to blame his American colleagues. He noted that if all the intelligence received by forces operating in Iraq was circulated, "they would have been overwhelmed." However, the inquiry said that failing to pass the intelligence on the earlier attack, was a reason for the loss of the Hercules. "...once airborne, the crew flew close to the Safire [surface-to-air] sites and crashed shortly afterwards."

The RAF aircraft had plotted a low-level route all the way to Balad, a massive US logistics base. They decided to do this instead of risking the short steep take-off, a period of flight deemed risky, but nevertheless performed at regular times.

Intelligence sharing in conflict zones is invaluable and efforts to stop similar situations arising again are underway. Air Vice-Marshal Iain McNicoll, Air Force Commanding No 2 Group said: "The

need for operational security for some operations is well understood but, in air operations particularly, there is a need to ensure that compartmentalisation of information does not lead to elements of the force operating in ignorance of vital information."

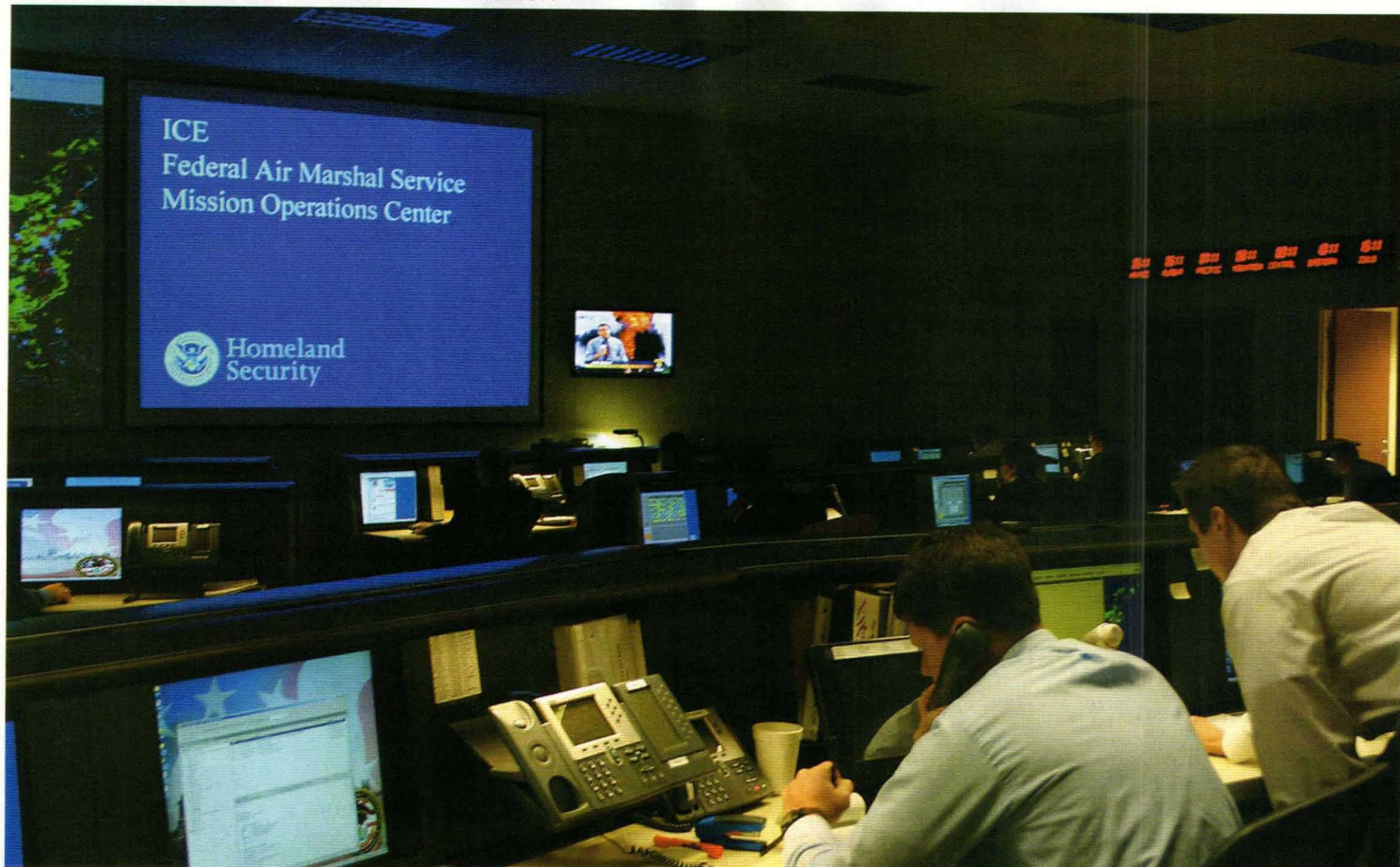


John Reid

© LEPL/STEVE MCMAHUS

The board of inquiry also mentioned several other contributory factors. It says that fire retarding technology - foam or inert gas - inside the fuel tanks, may have prevented an explosive fuel-air mix to develop. The fitting of a fuel tank "inerting system", which replaces oxygen with an inert gas like nitrogen to avoid explosions, "was being investigated as a matter of urgency," said Defence Secretary John Reid. The aircraft was also more vulnerable as it was flying low, "something now being avoided whenever possible," Mr Reid said.

- Since the conflict began, there have been nearly 900 surface-to-air attacks against Coalition aeroplanes.



VIPER SURVEILLANCE

New security teams coming to a ve

Just a couple of weeks after two US air marshals shot dead an American Airline passenger in Miami who said he was carrying a bomb in his rucksack, air marshals were involved in an undercover security programme that is built totally around exposing surveillance countermeasures and identifying suspicious characters, including terrorists. The Transportation Security Administration, (TSA) announced the move in December, and said teams of air marshals would begin counter-terrorism surveillance on land as part of a

"small test programme" that also involves un-uniformed police officers, bomb-sniffing dogs and transit inspectors. The operation saw surveillance operatives target airports, bus and train stations, transit intersections and maritime facilities.

The TSA's continuing security programme has seen the creation of Visible Intermodal Protection and Response teams, dubbed "VIPER" by those involved in its running. During the Christmas trial, Viper teams operated in numerous areas including alongside Amtrak train routes in California, ferry terminals in Washington state and the heavily used mass transit systems in Atlanta, Philadelphia and Baltimore. Viper personnel also went undercover inside the Washington Metro system and augmented on-going surveillance operations in New York and Boston.

It is believed an operational Viper team consists of two air marshals, two TSA security inspectors, a police officer, an

explosives canine team, and a TSA liaison officer. Mimicking the success of New York City high-visibility roaming Hercules teams, some Viper teams will don clearly marked TSA jackets; other teams, however, will not. As part of their duties, Viper plainclothes air marshals will mingle with members of the public waiting to board aircraft, trains, ships and highly populated areas related to transport. They will be looking for persons acting suspiciously or who may have been identified by other security services as 'persons of interest'. It is unknown at present just how many Viper teams will operate throughout the United States, but a TSA source said the air marshals were in place at seven major transport sites during the Christmas period.

A Viper team was surveilling crowds at Dulles International Airport, though officials deny this was as a result of a terrorist threat. Dulles is also one of the airports chosen to train dozens of

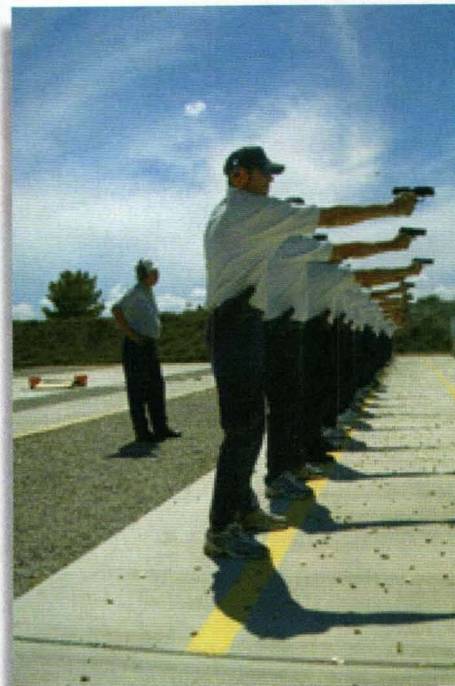




US AIR MARSHAL TRAINING

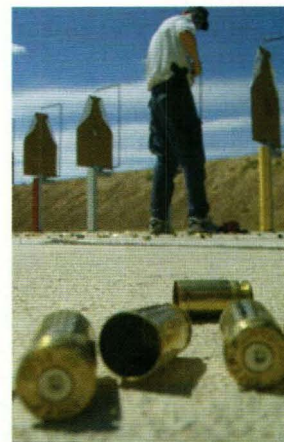
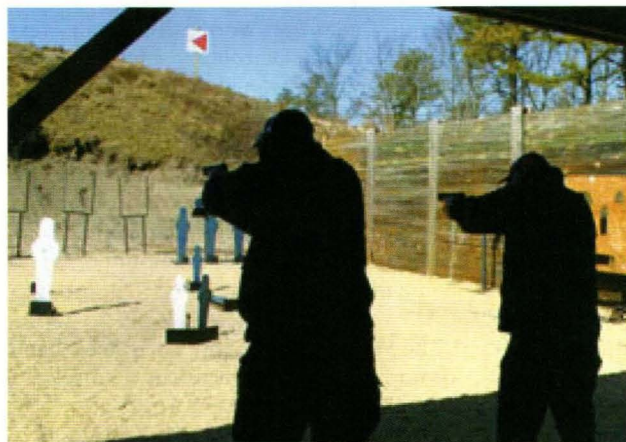
Every Federal Air Marshal candidate must successfully complete a two-phase training programme to fulfil the requirements necessary to become a US Federal Air Marshal (FAM). The initial phase consists of a seven-week basic law enforcement officer training programme conducted at the Federal Law Enforcement Training Center (F.L.E.T.C.) in Artesia, New Mexico. The FAM basic training has been specifically tailored to prepare recruits for the unique and critical mission of the Federal Air Marshal Service. The core curriculum taught during FAM basic training is drawn from the following disciplines: constitutional law, basic marksmanship, physical fitness, defensive tactics, emergency medical and fundamental law enforcement investigative/administrative practices. FAM candidates who successfully complete the basic training curriculum continue to Phase II training conducted at the William J. Hughes Technical Center in Atlantic City, NJ.

Phase II training is dedicated to providing FAM candidates with the knowledge, skills and abilities specifically applicable to the environment in which they will perform their duties. Emphasis is placed on developing advanced firearms and defensive techniques proficiency, advanced operational tactics, strength conditioning and aerobic training, aircraft



ANCE

ue near you?



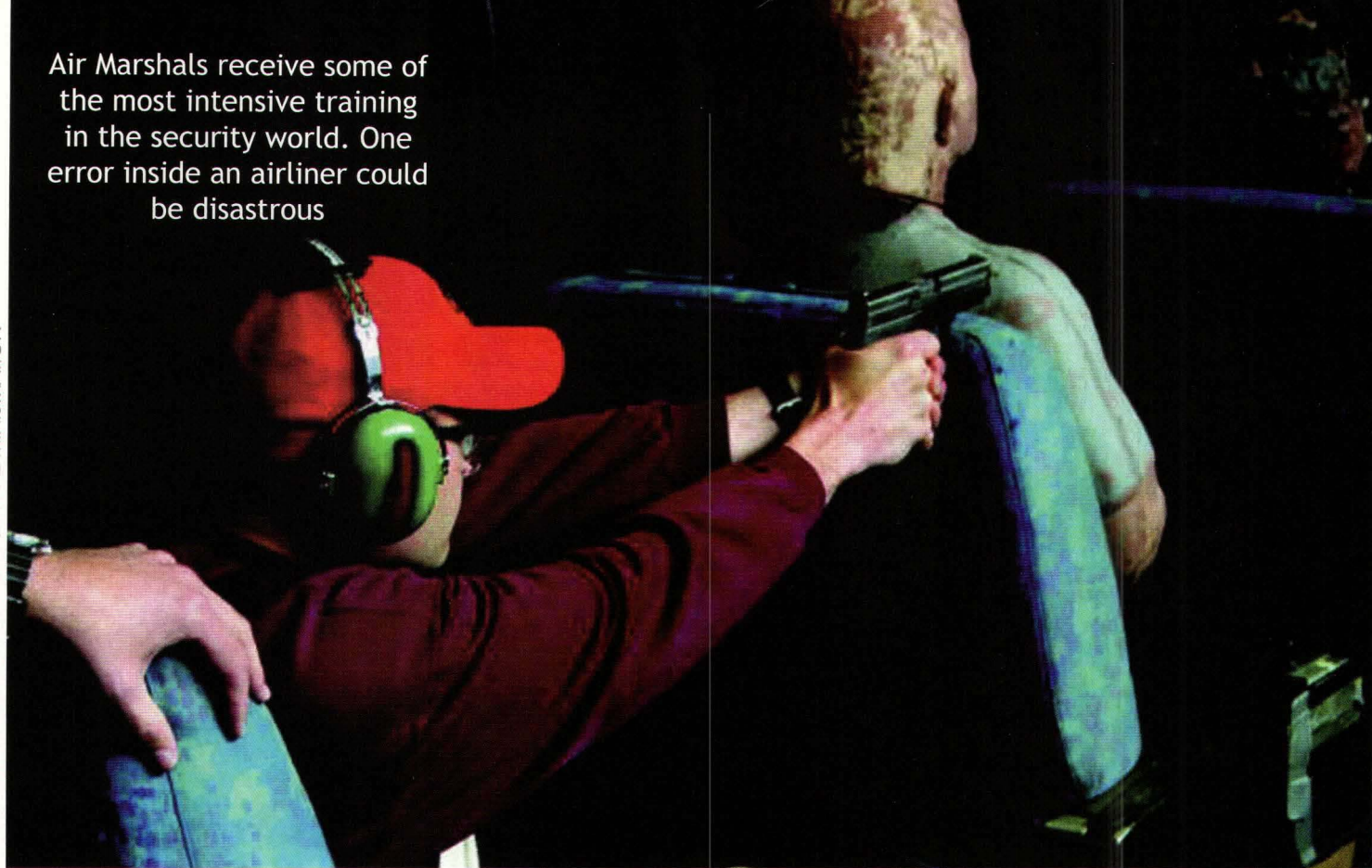
systems emergency procedures and legal and administrative protocols. Candidates who successfully complete Phase II have demonstrated the ability to carry out the duties and tasks necessary to fulfil the mission of the Federal Air Marshal Service. Upon graduation from Phase II, newly appointed Federal Air Marshals are assigned to one of 21 field offices to begin flying missions.

“observers and screeners” in “behaviour recognition techniques.” As part of their intensive training, air marshals have already undergone training in this specialist area. An Eye Spy intelligence source said: “Air marshals are fully conversant with identifying suspicious activity. A great deal of their work involves noting people who could be employing countermeasures. This is a difficult task, and will inevitably lead to innocent folk being stopped and questioned. However, with additional training and a number of very interesting techniques being re-

searched already, the chances of surveillance errors will be minimal. It makes sense to use air marshals in this environment. They have already proved their worth in several instances and their experience should augment the Viper initiative.”

By going public with the Viper programme, the TSA is confident that the public will react positively to another line of security. “TSA is going to extend its outreach into other modes of transportation,” said David Adams, spokesman for

Air Marshals receive some of the most intensive training in the security world. One error inside an airliner could be disastrous



A potential air marshal gets to grip with a 'terrorist' in pre-assignment training

the Federal Air Marshal Service. "We think this is a very good approach to test our tools and quickly deploy resources in the event of a situation or a threat. It shows we could be at any of these places."

As security has been tightened on public aeroplane flights, some regulations regarding the carrying of sharp items on board flights have been relaxed. Items such as small scissors will now be allowed in carry-on luggage. This, however, is still at the discretion of the screener and airline security. These "screeners and observers" are being trained using techniques once used only by the intelligence services. Officials at Los Angeles,

Miami, Dallas-Fort Worth, Cincinnati, New York, Houston, Detroit and Chicago will be taking more than a casual glance at persons showing high stress levels, anxiety, sweating, avoiding eye-contact or deception. Of course in many cases stress levels and anxiety do rise prior to boarding aeroplanes, but the training methods currently being employed should overcome most problems.

The Viper initiative appears to have been prompted by the air marshals themselves who are keen to play a more active surveillance role beyond the confines of the aircraft. "Air marshals are trained to covertly detect potential criminal terrorist

pre-attack surveillance and other suspicious activity," states a TSA memo written by Patrick F. Sullivan, deputy assistant director of TSA's Federal Air Marshal Service flight operations office. Air marshals assigned to support the VIPR team will also be looking for individuals attempting to avoid or depart areas upon visual observation of the VIPR teams."

During a flight air marshals regularly record and note unusual or suspicious activity. Once the aeroplane had landed successfully, many people believe the air marshal's assignment is over. However, that is not necessarily the case. Air marshals will forward comments to

An Air Marshal's Worst Nightmare

Security for all forms of transport is provided for by several different departments. However, airline security is far tighter than for other modes of transport. Checks are often carried out on passenger lists and luggage and documents are checked thoroughly. Passengers are also invited to pass through electronic devices for screening. Adding surveillance to airports prior to boarding will augment security. Needless to say some people still attempt to take weapons into the cabin. These images show how an electronic radio device was used to attempt to get a gun on board a flight at Austin-Bergstrom International Airport in Austin, Texas.





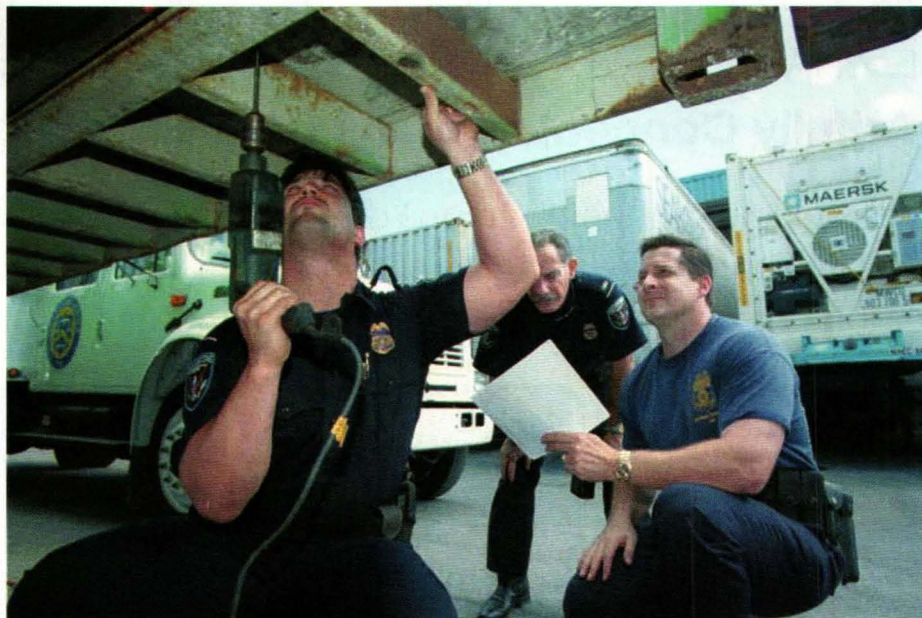
airport security who may wish to continue surveillance once the aeroplane has landed.

Not everyone is happy at the Viper programme. Some security advisors note that the training afforded to air marshals is meant for use predominantly on-board aeroplanes. "In one word, this is absurd," to put air marshals in bus and train stations, said Doug Laird, a security consultant and former head of security for Northwest Airlines. "This is clearly a responsibility of the local jurisdictions. They don't have enough air marshals to carry out the mission they are supposed to do. To spread them even thinner dilutes the reason they are there in the first place." American Airlines pilot Denis Breslin, spokesman for the airline's pilots' union, agreed and said air marshals ought to stick to airplanes. "I don't think there's enough air marshals to cover commercial aviation as it is," Breslin said. "That's what transit police are for."

Laird's comments were rejected by most air marshals. David Adams said "marshals are the law enforcement arm of the TSA, which is charged with overseeing all modes of transportation - not just aviation. This is part of our responsibility to assist in the non-aviation domain. The whole purpose is that people will not know when we're going to be there or if we are going to be there. It's a preventative approach."

THE BRIEFING ROOM ➤

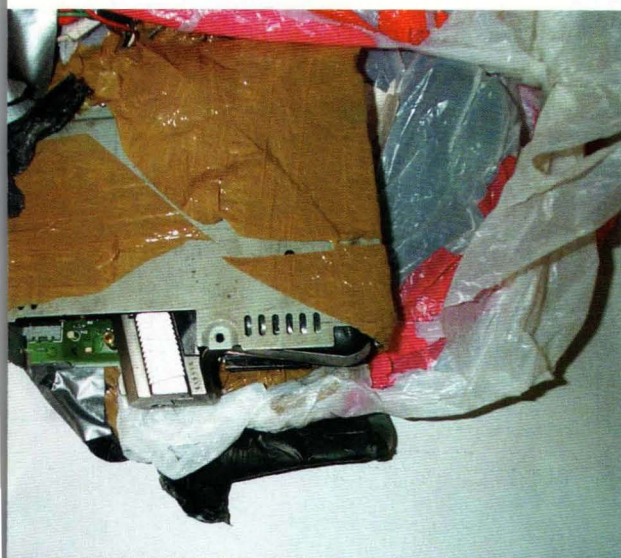
Surveillance Detection System: Tactical Information Sharing



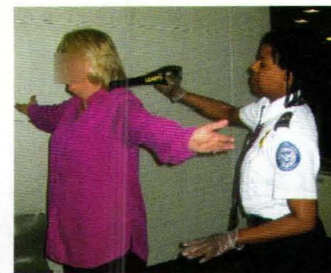
The Federal Air Marshal Service (FAMS) has taken a giant step forward in the fight against terrorism with the development of the Surveillance Detection System (SDS). The SDS is a Tactical Information Sharing System that captures Federal Air Marshal observations of suspicious activity in the aviation domain, analyses the data and shares it with other agencies. SDS has the potential to revolutionize conventional investigative information sharing. Federal law enforcement has learned that some form of "surveillance" by the perpetrators precedes significant criminal or terrorist acts, particularly in terrorist activities. SDS enables Federal Air Marshals (FAMS) in the field to report the surveillance of suspicious behaviour and activity instantly into a database for analysis, and provide an information source for examining long-term trends and patterns. With this information, FAMS are equipped to stop criminal or terrorist acts when they are most vulnerable - in the planning stages of an operation.

FAMS can send Surveillance Detection Reports (SDRs) and view previously entered SDRs via their PDAs. The FAMS' Tactical Information Branch (TIB) receives the SDRs that are entered directly into the database. This collection of SDRs then becomes an invaluable investigative resource. FAMS in the field have direct access to the database.

The TIB analyst's are developing, cataloguing, associating, categorizing, and maintaining database of suspicious trends and tactics, leading to the identification of terrorist surveillance activities that is being shared with the Federal law enforcement community.



BRIEFING ROOM

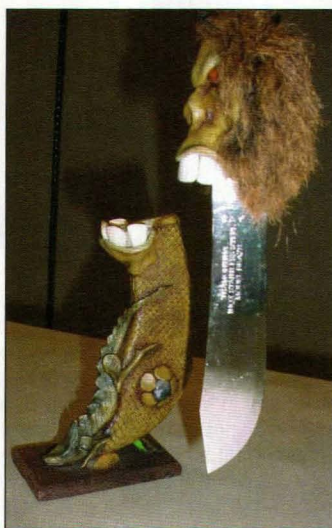


Artfully Concealed Items Confiscated by TSA Screeners

This selection of photographs of artfully concealed weapons were discovered by TSA Screeners during recent security searches. If anything these images emphasize the need for continued vigilance at airport checkpoints



Statue upright on table



Statue with blade exposed



Statue lying on side with blade exposed

A statue artifact concealing a sword found at the security checkpoint by a TSA Screener at Luis Munoz Marin International Airport in San Juan, Puerto Rico.

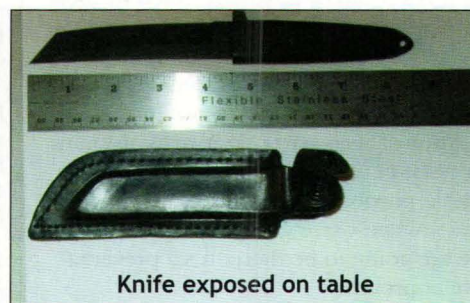
Second sword



Carseat hiding knife



Knife inside carseat



Knife exposed on table

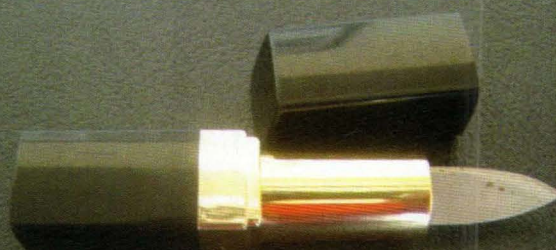
This set of photos illustrates a child's car seat used to conceal a knife that was confiscated at Eppley Field Airport in Omaha, Nebraska.

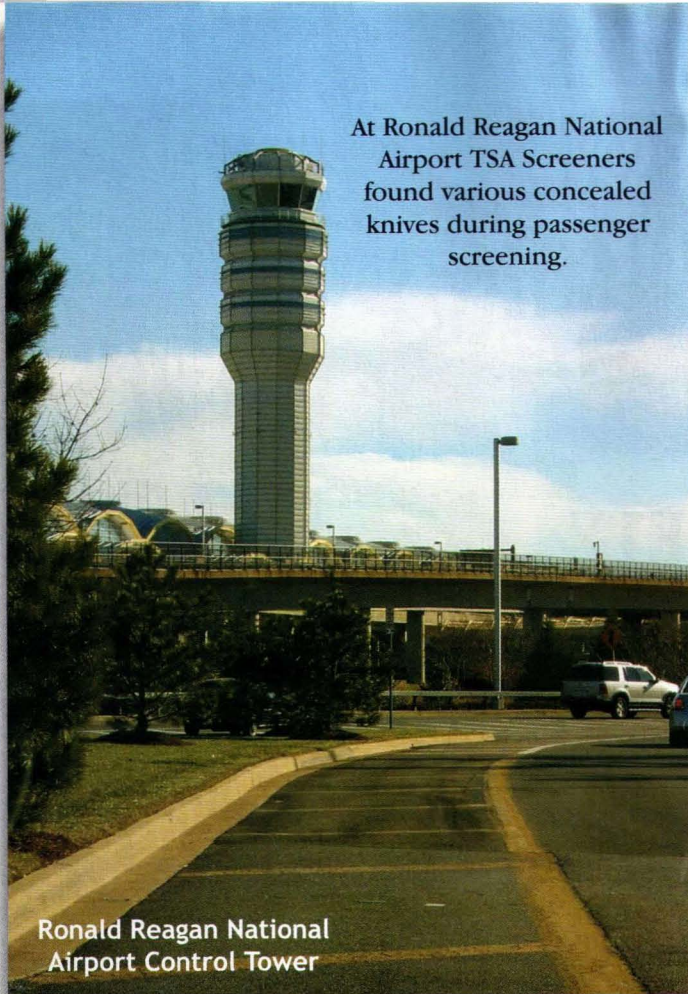
TSA Screeners at Minneapolis International Airport found these prohibited items that were confiscated at the security checkpoints.



Knife Pen

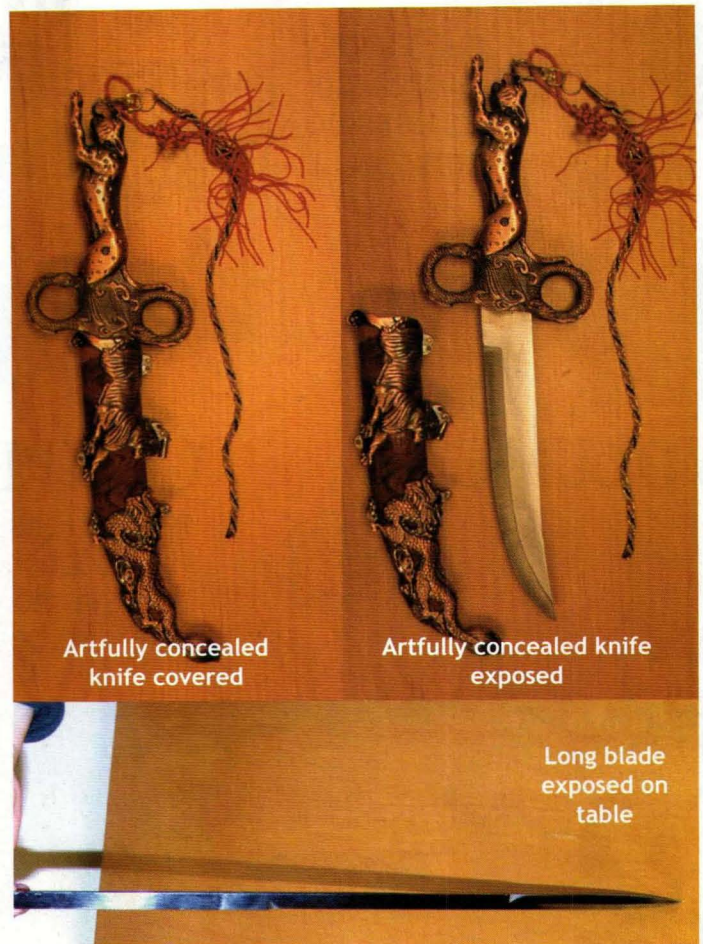
Lipstick Knife





At Ronald Reagan National Airport TSA Screeners found various concealed knives during passenger screening.

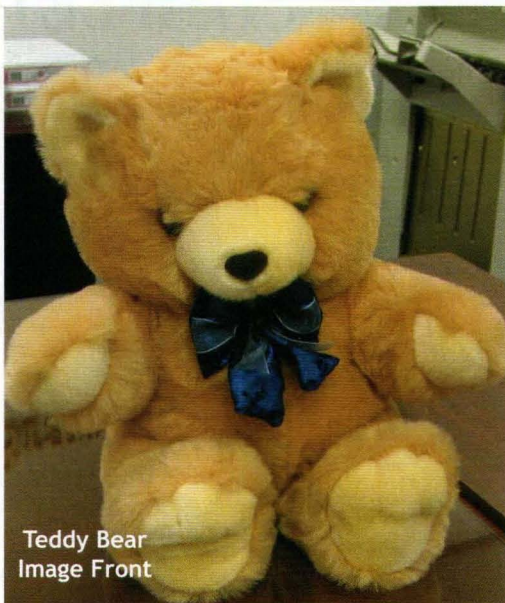
Ronald Reagan National Airport Control Tower



Artfully concealed knife covered

Artfully concealed knife exposed

Long blade exposed on table

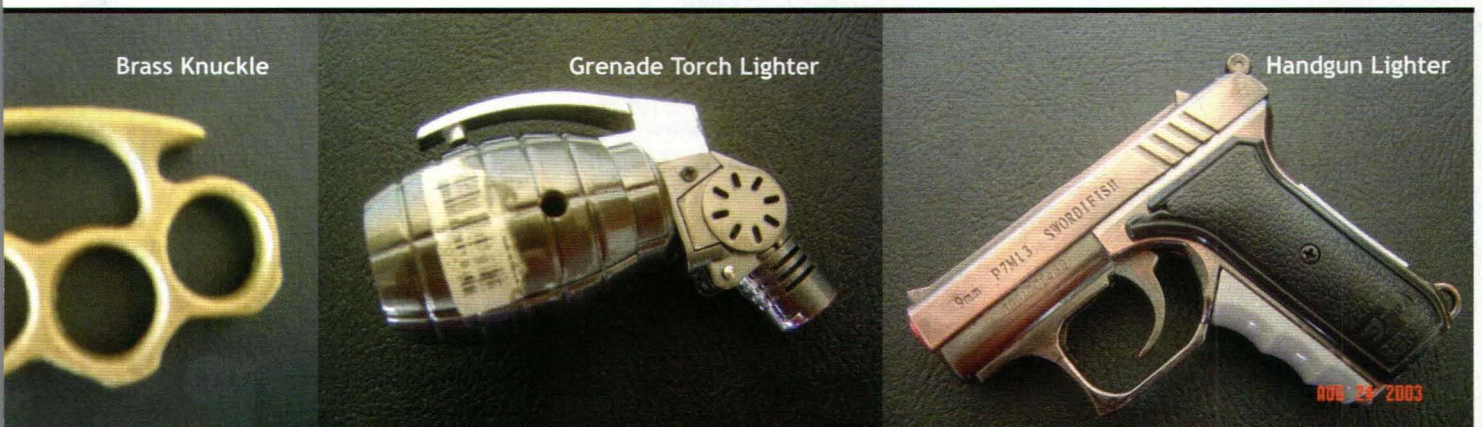


Teddy Bear Image Front

TSA Screeners in Orlando discovered a loaded handgun stuffed inside a plush teddy bear as it was being x-rayed the morning of 12 July 2005. The bear belonged to a 10-year-old boy who received it as a gift from a stranger



Teddy Bear Image Back



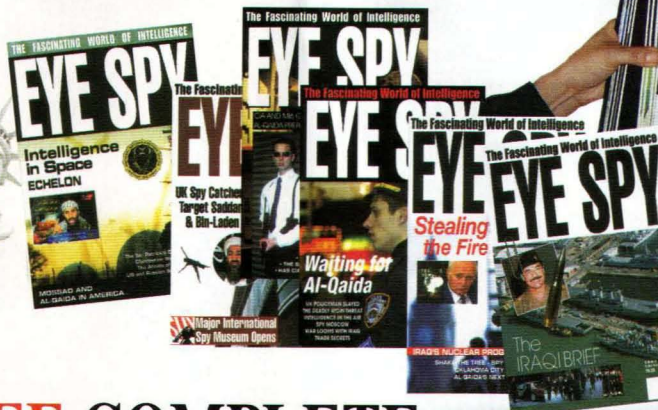
Brass Knuckle

Grenade Torch Lighter

Handgun Lighter

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.eyespyimag.com



French intelligence placed blame for sinking of Rainbow Warrior on MI6

Documents obtained under the Freedom of Information Act reveal French intelligence officers, supported by officials in Paris, conjured up a covert media disinformation campaign that would divert attention and suspicion away from France's involvement with the sinking of Greenpeace vessel, the Rainbow Warrior in 1985. The scam was discovered by MI6, but unable to comment publicly, an "infuriated" Prime Minister Margaret Thatcher ordered Whitehall officials to force Paris to shut down the DGSE operation.

Eye Spy has learned that the plan was devised months prior to the sinking of Rainbow Warrior, after DGSE (Direction Generale de la Securite Extérieure) officers who had infiltrated Greenpeace, also discovered an MI6 agent amongst its ranks. According to

intelligence sources, MI6 had used a front company to obtain information on the movements of Rainbow Warrior and its "protest agenda."

Rainbow Warrior had been despatched to New Zealand in July 1985 to monitor controversial French nuclear tests near Moruroa. When the ship arrived, DGSE operatives were waiting in Auckland armed with explosives and orders to sink the ship. The plan was duly carried out and the Rainbow Warrior was crippled. Greenpeace photographer Fernando Pereira was killed in the blast.

New Zealand police soon demanded the arrest of several people, unbeknown at the time, all of them were connected to the DGSE. Some intelligence officers, including Christine Cabon, a former French Army officer, had already left the country. She had

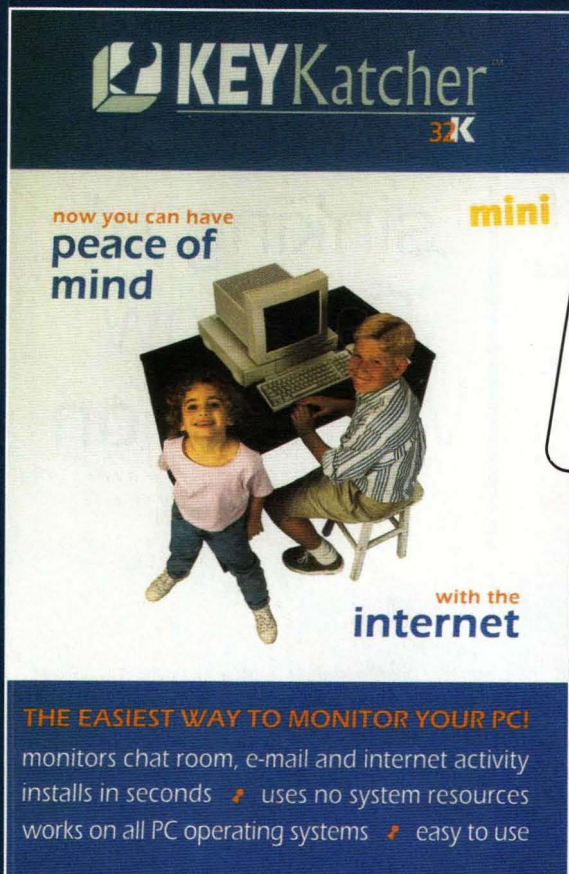


MI6 and DGSE Spy Games

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.



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

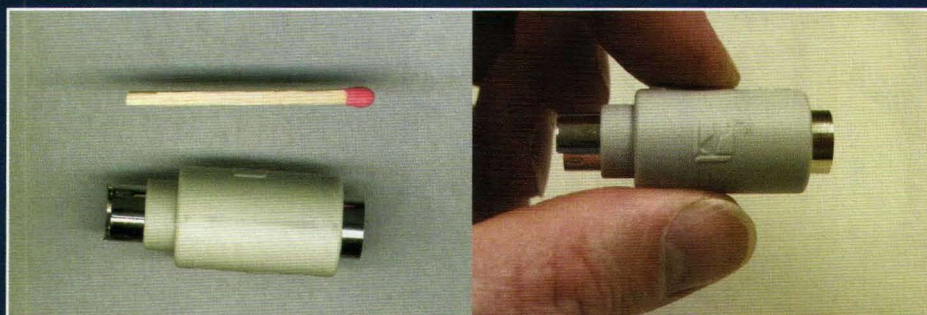
IBM PC compatible computer
(Windows 98, 95, NT Linux)

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.

Five various-size KeyKatchers 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



successfully infiltrated Greenpeace's New Zealand office and provided information to the captains of two French vessels Ouvea and Turenges. These ships were participating in the Moruroa tests. New Zealand security officials learned she was in Tel Aviv and asked that police arrest her. However, Cabon was tipped off by Paris and she duly disappeared before an arrest could be made - as did a number of other agents. Cabon's whereabouts are still a mystery 20 years on. Since then, at least eight DGSE officers, including some experienced divers, have been identified and named in the destruction of the Rainbow Warrior.



Prime Minister Thatcher

The active DGSE team was supported by a group of senior analysts who believed they had covered all eventualities in the event France's involvement would be discovered. When suspicion fell on the intelligence agency, the released 2005 documents show that Paris authorised the 'MI6 disinformation plan'. Unbeknown to French president, François Mitterrand, British intelligence had more than a scent that the DGSE was passing spurious information to their agents who covertly fed the French media. At the time, of course, MI6, who



EYE SPY

Some of the DGSE officers involved in the affair

were themselves monitoring Greenpeace, decided to exert underground diplomatic pressure on the DGSE, for the Rainbow Warrior incident was threatening to spiral out of control and damage Anglo-French relations. London ministers were advised that Mitterrand, "was in danger of being toppled." Sir John Fretwell, the British ambassador in Paris in a memorandum wrote: "The highest personalities in the land are fighting for political survival and even the fabric of the state is beginning to shake under the impact of repeated revelations, denunciations, attempts to acknowledge bits of truth while concealing others and the desperate attempts to find answers which will somehow satisfy public opinion while keeping the president above the melee." This did not stop Thatcher instructing officials to "go after Paris."

The French media, 'armed' with the DGSE disinformation claimed that MI6 had sunk the Rainbow Warrior in "order to discredit France." One newspaper even claimed an MI6 front company had sold the dinghies (used to attack the vessel) to the DGSE and had "prior knowledge" of the sabotage operation.

The Sunday Times told the Foreign Office that "French official sources were briefing freely anyone who would listen about British involvement in the sinking

Continued on page 82

Christine Cabon, a former French Army officer, alias Frederique Bonlieu Cabon infiltrated the Greenpeace New Zealand office in the spring of 1985. Her mission was to uncover plans for the Moruroa trip and gathered directions, maps, and information for the crew of the *Ouvea* and *Turenges*, two French vessels. Cabon departed New Zealand weeks after successfully passing intelligence to her colleagues. When the Warrior was sunk, she was in Tel Aviv. Within hours however, Auckland police had discovered her location and asked Israel to arrest her. However, Paris had already advised her to leave and no arrest was made. Today, the whereabouts of Cabon are still a mystery. It is almost certain that the DGSE used the *Ouvea* to smuggle explosives, an inflatable and an outboard motor into New Zealand. One of several persons on board was a Dr Xavier Maniguet, a doctor specializing in treating diving accident victims. When arrested, he insisted he was only a passenger. He later wrote a book, *The Jaws Of Death (Shark As Predator, Man As Prey)*. The book made a small comment on the Rainbow Warrior bombing.

Petty Officer Bartelo, alias Jean-Michel Berthelot was also a combat frogman. His whereabouts since the bombing are unknown.



Bartelo

Petty Officer Gerald Andries, alias Eric Audrenc, also a diver. Whilst in London, he purchased the inflatable and the outboard motor used in the bombing. Andries joined the French army in 1975 and later became a DGSE officer based at the Navy Frogmen Training Centre

in Corsica. In 1991, Andries was arrested in Basel. He crossed into Switzerland on the Brussels-Milan Eurocity train without a passport. Interpol were alerted and informed the police that an international warrant was outstanding for his arrest. He was detained in prison in Basel while the Swiss authorities awaited an extradition request from New Zealand. On December 17 the New Zealand government informed the Swiss authorities that they would not be seeking Andries' extradition.



Gerald Andries

Major Alain Mafart, alias Alain Turenge, was a DGSE officer and deputy commander of the Navy Frogmen Training Centre in Corsica. He supported the team and was apprehended by New Zealand police when returning a rental van. He didn't waste time and pleaded guilty to manslaughter and was sentenced to 10 years imprisonment in 1985. Following a United Nations sponsored mediation between New Zealand and France in July 1986, Mafart was deported to the island of Hao in French Polynesia to serve just three years. In December 1987, Mafart was sent to France, after complaining of stomach pains. He never returned to finish the rest of his sentence. One year later he joined a two-year course at the Ecole de Guerre (Military College) in Paris. Mafart was promoted to colonel



Alain Mafart

in December 1993. According to the French newspaper, *Le Monde*, He was serving near Paris on a base housing several command staffs, including that of military intelligence.

Captain Dominique Prieur, alias Sophie Turenge, was a DGSE officer and Christine Cabon's controller. She was a specialist in European peace organisations. After her arrest by New Zealand police, she pleaded guilty with Mafart to reduced charges of manslaughter and was sentenced to 10 years imprisonment in 1985. Because of the UN ruling in the arbitration between New Zealand and France (July 1986) she was deported to the island Hao (French Polynesia) to serve three years instead. On 6 May 1988 she returned to France because she was pregnant.



Dominique Prieur

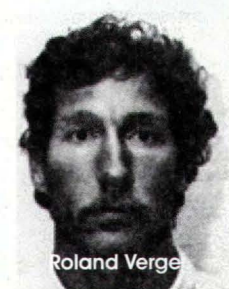
Colonel Louis Pierre Dillais, alias Jean Louis Dormand Dillais was the DGSE operational head to stop the Rainbow Warrior protesting. A senior officer at the underwater combat centre at Aspretto in Corsica, Dillais travelled under the assumed name of Jean Louis Dormand and reportedly drove the inflatable boat for the two divers who planted the bombs on the ship. After the bombing, he tried to cover all tracks by sending the divers to the South Island of New Zealand. He disguised himself as a tourist in Queenstown until he flew to Australia on 23 July. In 1994, French Defence Minister Francois Leotard appointed Dillais as chief of the private office of the Minister of Defence, effectively the head of military intelligence.

Previously, Dillais worked for the general secretariat of the 'Defense National', attached to Prime Ministerial Services, in charge of European-Atlantic affairs. Many analysts believe Dillais failed to protect his unit. They were arrested and identified. Some believe Dillais should have resigned quickly, but are convinced his career has been protected because his father-in-law is none other than former foreign affairs minister Jean Francois Poncet.

A third DGSE 'back-up' team was also identified. Some analysts, however, believe it was this team that planted the explosives - **Alain Tonel, Jacques Camurier, Francois Verlet**. Verlet left for Tahiti on 10 July. Tonel and Camurier crossed to the South Island on 11 July with Dillais (Dormand) before leaving the country.

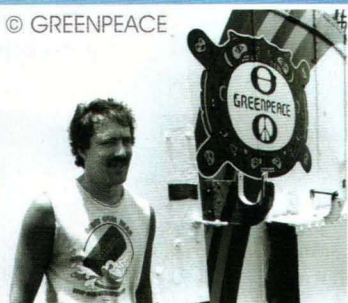
Colonel Jean-Calude Lesquer, was head of the action unit charged with the Rainbow Warrior bombing. He lost his post over the scandal but a few years later was promoted to Brigadier-General because of his performance in the first Gulf War. In 1995 he was promoted to Major-General, and assigned to COFRAS, a loose official group that concludes major contracts between French arms manufacturers and foreign governments.

The Captain of the Ouvea was Chief Petty Officer Roland Verge, alias Raymond Velche, a military diver who joined the French Army in 1970 and later the DGSE. He was based at the Navy Frogmen Training Centre (CINC) at Aspretto in Corsica. This was closed just months after the failed operation.

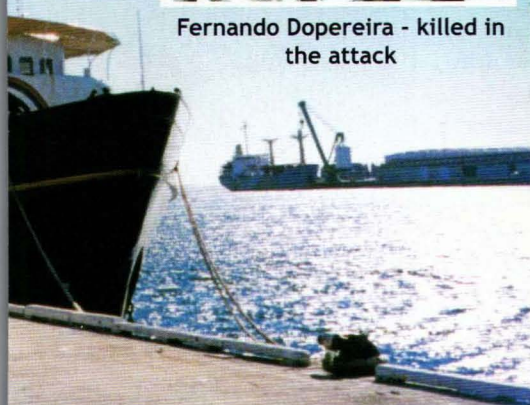


Roland Verge

© GREENPEACE



Fernando Dopereira - killed in the attack



FBI Still Searching for the 'Anthrax'

The fourth anniversary has come and gone since Bob Stevens, a British picture editor for American Media Inc., who had settled in Florida became the first of five victims after coming into contact with Ames - a weapons grade strain of anthrax. At the time, the FBI were fairly convinced terrorism was involved, though the bureau's opinion has changed often and many officers remain open-minded. The public could not have imagined that four years later no-one has been charged with the crime of sending anthrax-laden envelopes in the post. The death of Mr Stevens sparked a huge international manhunt, and while the anthrax source has been traced, the identity of the killer dubbed the 'anthrax man'



Bob Stevens became the first fatality in the anthrax affair

remains as elusive as Jack the Ripper.

Within weeks of Mr Stevens death, four other people were dead, including three postal workers. A further 17 became ill but survived.

The FBI team assigned to the investigation initially numbered over 30, but this has dropped to 20 as leads and avenues for exploration slowly run out. Officers have interviewed 8,000 people and have subpoenaed a further 5,000, though new suspects are at a premium, and intelligence watchers believe that the chances of ever learning the identity of the murderer are ebbing away. However, the public is still being urged to pass on any information via a dedicated FBI link on its web page.

Besides the hunt for the anthrax man on US soil, the bureau's

investigation has spanned several countries, and has included the interrogation of al-Qaida suspects detained in Afghanistan and Guantanamo Bay. This was because some of the letters contained references to al-Qaida's attack on New York and Washington DC.

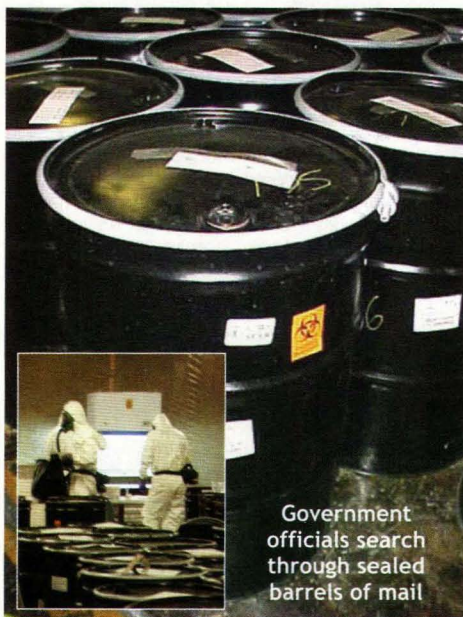
The letters were posted between 18 September and 9 October 2001 to publishing houses and senior Washington politicians, including Tom Daschle and Patrick Leahy. As they entered the postal system, some of the packages leaked and contaminated sorting houses. The FBI discovered anthrax on Mr Stevens computer keyboard, indicating he had anthrax on his hands after opening an envelope.

Mr Stevens death, coming so soon after 9/11, caused panic and fear throughout the United States. It was a particularly worrying time for postal workers. Numerous buildings were closed and specialist chemical emergency teams were called regularly to examine suspect packages. In most cases it was a false alarm, but valuable time was lost. Combined with dozens of deliberate hoaxes, the security services were stretched.

It did not take long for analysts to determine the anthrax was of a unique strain, and the hunt was on to pinpoint where it was manufactured, stored or stolen. The strain was discovered in a dead cow in Texas in 1981, and sent to the US Army Medical

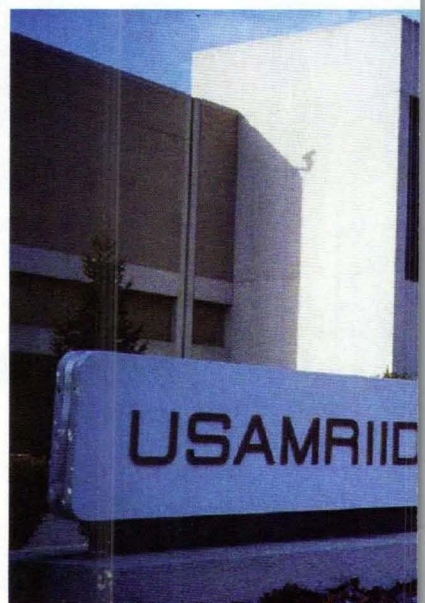


Research Institute for Infectious Diseases (USAMRIID) in Fort Detrick for study. At the time, only four countries were known to have quantities of the Ames strain used in the attacks. One of those nations was Iraq and initial attention was focused on Baghdad. As the investigation moved on, Iraq was ruled out and investigators began looking more closely at the real possibility the terrorist[s] were home-grown.



Government officials search through sealed barrels of mail

COURTESY: FBI

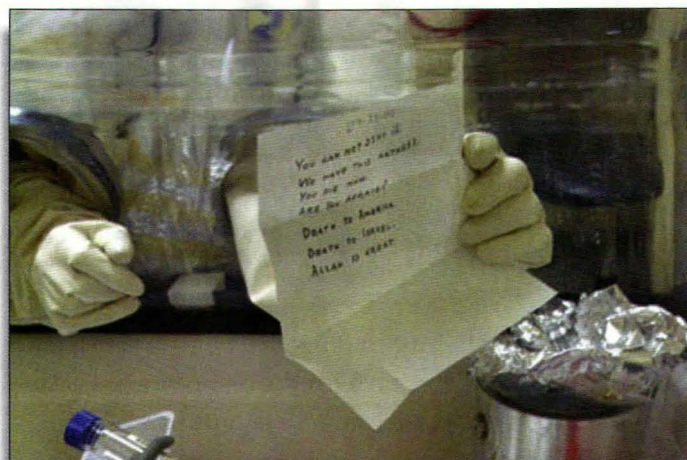


ng Man'



observance - Steven Hatfill (above) an American bio-defence worker who worked at the facility between 1997 and 1999. He has never been charged - but was put under surveillance. Ultimately, Hatfill filed a legal action against the bureau for "harassment".

In 2003, the FBI were again at Fort Detrick, this time officers spent three weeks draining a nearby pond after a tip off that the a case of anthrax had been dumped in the water. A massive search yielded no clues. It is unclear whether investigators were



searching for clues into the 2001 anthrax attacks, or an incident which occurred in 1992, when 27 sets of specimens, including the Ames strain were reported missing at Fort Detrick after officials conducted a stock check. US Army officials also found evidence that an employee was secretly entering one laboratory in the middle of the night to "conduct unauthorised research, apparently involving

anthrax." As for the lost samples, officials have always said they "posed no threat."

WESTWIND 99

The FBI was never ignorant to the possibility that terrorists may one day attack using bio-weapons such as anthrax. In 1999, it conducted a training operation codenamed WESTWIND 99 in conjunction with the security services in

Los Angeles. Westwind 99 simulated a chemical attack on a local air show by a fictional domestic terrorist group, resulting in the simulated deaths of 2,000 victims. The exercise was all-inclusive, encompassing the pre-investigation phase, detecting the possibility of a terrorist attack, through a comprehensive consequence management response, an investigative response, and finally culminating in the tactical arrest of the "terrorists."

Despite having the mechanism in place and investigative procedures enabled to find the attackers, the Anthrax Man remains as elusive as ever.

Maureen Stevens, the widow of Robert, is now on the verge of suing the US Government for \$30 million, alleging security at USAMRIID was poor.

Timeline of Anthrax Attacks

2 October 2001: Robert Stevens, is hospitalised after inhaling anthrax.

5 October 2001: Robert Stevens dies.

8 October 2001: Officials reveal second American Media Inc. employee Ernest Blanco, 73, has tested positive for anthrax infection.

12 October 2001: NBC's Tom Brokaw's assistant Erin O'Connor revealed to have had exposure to anthrax. New York City woman contracts exposure to anthrax opening mail.

13 October 2001: Five American Media Inc. employees test positive for exposure to anthrax.

15 October 2001: Letter received by US Senator Thomas Daschle, contains anthrax. Infant



son of an ABC news producer contracts 'skin form' of anthrax. Letter was originally opened on 25 September. Doctors confirm Ernesto Blanco has skin anthrax.

17 October 2001: Anthrax discovered in Governor George Pataki's office. Thirty people at Capitol Hill test positive for exposure to anthrax.

18 October 2001: Former CBS News anchor Dan Rather's assistant and a postal worker handle mail containing the anthrax virus. A New Jersey postal worker tests positive for cutaneous anthrax.

19 October 2001: A second New Jersey postal worker tests positive for skin anthrax.

20 October 2001: Two US postal workers in Washington DC die from inhalation anthrax.

22 October 2001: A third postal worker in Washington tests positive for inhalation anthrax.

23 October 2001: Anthrax discovered in mail centre near White House.

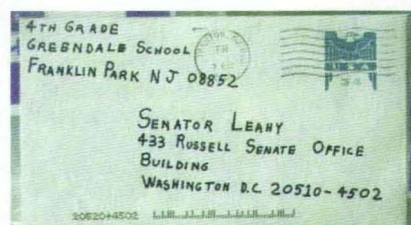
24 October 2001: Six Washington DC postal workers hospitalised for suspected anthrax.



Governor George Pataki

25 October 2001: Anthrax found in another part of the Hart Senate Office Building.

31 October 2001: Hospital worker in New York dies becoming the fourth fatality of inhaled anthrax since 11 September.



ORS

the past

experts said: "What these photographs disguise is the vastly different characters of the former DGs." Professor Andrew, who was appointed by the government to write MI5's official history, said he believes Sir David Petrie, who is pictured for the first time and who battled long and hard against Hitler's spies, was "one of the best heads."

MI5 also feature Sir Roger Hollis. He headed the service between 1956 and 1964. There were allegations that Sir Roger was a Soviet spy, though these have never been proven. Only four former heads are still alive.

LINKS

www.mi5.gov.uk/output/Page417.html

He oversaw one of the busiest periods in the Service's history, during which the Service carried out many successful intelligence operations against Nazi Germany.

Sir Percy Sillitoe
(1888-1962)
4th Director General,
1946-1953



Like his predecessor, Sir Percy came from a police background. He served as Chief Constable of a number of constabularies before becoming the Security Service's Director-General in 1946.

During his time in office, he faced the post-war rise in Soviet and Communist spying and subversion in the UK, including the exposure of the Cambridge spy ring.

He became the first former Director General of the Service to publish an autobiography, *Cloak without Dagger*, in 1955.

Sir Dick White
(1906-1993)
5th Director General,
1953-1956

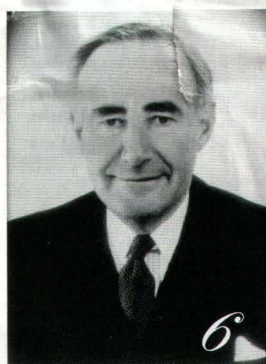
Sir Dick was a career Service officer, having joined in the 1930s. During the Second World War he was closely involved in operating the highly successful "Double Cross" system against Nazi Germany.



He became Director General in 1953 but in 1956 moved across to the Secret Intelligence Service (SIS) to become its chief. He headed the SIS until his retirement in 1972 and remains the only person to have headed both organisations successively.

Sir Roger Hollis
(1905-1973)
6th Director General,
1956-1965

Sir Roger joined the Service in 1936 following an earlier career as a businessman. He was appointed Deputy Director General in 1953 and



Director General in 1956, serving in that capacity for nine years.

In 1981, allegations were published claiming that Sir Roger had been a Soviet secret agent. These were investigated and found to be groundless.

(see www.eyespymag.com for further information)

Sir Martin Furnival Jones
(1912-1997)
7th Director General,
1965-1972



Sir Martin qualified as a solicitor before joining the Service in 1938. He served with distinction during the Second World War, working in a variety of roles at the Supreme Headquarters, Allied Expeditionary Force (SHAEF) and the War Office.

He became Director General of the Service in 1965 and retired seven years later.

Sir Michael Hanley
(1918-2001)
8th Director General,
1972-1978

Sir Michael served as an officer of the Royal Artillery during the Second World War, subsequently becoming the Assistant Military Attaché in

Budapest in 1946. He joined the Security Service in 1948.

He became Deputy Director General in 1971 and was promoted to Director General the following year.



Sir Howard Smith
(1919-1996)
9th Director General,
1978-1981

Sir Howard joined the Service after a long and distinguished career with the Foreign and Commonwealth Office.

During his 32 years in the Foreign Service he held a variety of posts, including serving as the British ambassador to Czechoslovakia and the Soviet Union.

He became Director General of the Security Service in 1978.



Sir John Jones
(1923-1998)
10th Director General,
1981-1985

Sir John was a former officer in the Royal Artillery and served as a civil servant in the pre-independence Government of Sudan. He joined the Security Service in 1955.



He became Deputy Director General in 1976. He succeeded Sir Howard Smith as Director General in 1981.

In 1983, he was appointed Knight Commander of the Order of the Bath (KCB) by HM The Queen.

Sir Antony Duff
(1920-2000)
11th Director General,
1985-1987



Like his predecessor-but-one, Sir Antony had a distinguished diplomatic career before joining the Service as its Director General. He served in a variety of high-profile roles with the Foreign and Commonwealth Office, serving as the last Deputy Governor of Southern Rhodesia (now Zimbabwe) before its independence in 1980.

He subsequently became Deputy Secretary at the Cabinet Office before moving to the Security Service, which he headed for two years.

Continued over

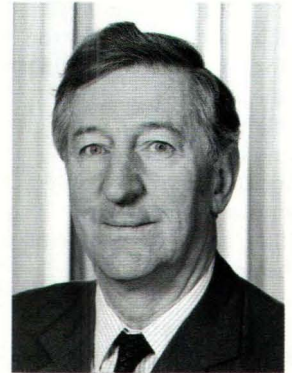
HALL OF MIRRORS



Sir Patrick Walker (1932-)
12th Director General, 1987-1992

Sir Patrick joined the Security Service in 1963, following a period of service in the pre-independence government of Uganda.

He became Director General in 1987, overseeing the Service's transition through the end of the Cold War before his retirement in 1992.



Dame Stella Rimington (1935-)
13th Director General, 1992-1996

Dame Stella was the first woman to become Director General of the Security Service and in 1993 became the first publicly acknowledged DG. She joined the Service in 1969 and worked in a variety of roles, including counter-subversion and counter-terrorism.

She was appointed Dame Commander of the Order of the Bath in 1996 and published her autobiography, *Open Secret*, in 2001.



Sir Stephen Lander (1947-)
14th Director General, 1996-2002

Sir Stephen joined the Service in 1975 and became Director General in 1996, serving in that capacity until his retirement from the Service in 2002.

He subsequently became the Law Society's Independent Commissioner.

In 2004 he became the Chairman-Designate of the Serious Organised Crime Agency, a new body which is due to become operational from 1 April 2006.



© Crown Copyright

100% SECURE
Superb new easy to use shopping cart!

24 Hours a Day

www.eyespymag.com

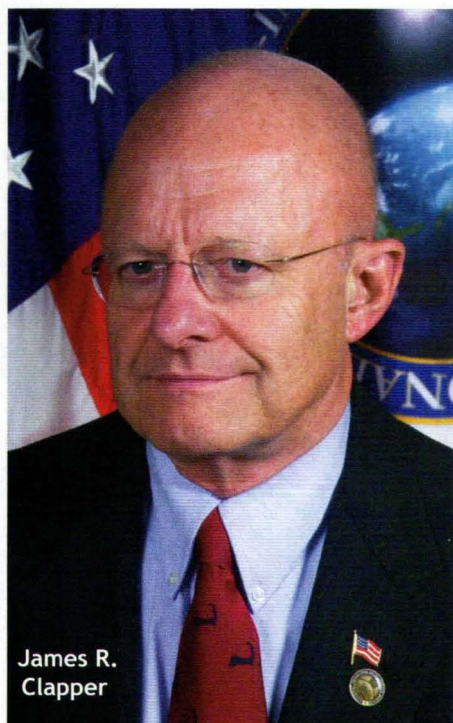
BRAND NEW WEB SITE AND SHOPPING AREA - 100s OF NEW PRODUCTS

FIVE MILLION HITS A MONTH

One of the US intelligence communities most secretive organisations, the National Geospatial-Intelligence Agency (NGA), is the latest 'intel gem' to feel the force of change sweeping through America's huge intelligence machine.

After a major reshuffle which has seen the United States primary intelligence agencies pinned under the umbrella of a national intelligence supremo, the NGA's director, James R. Clapper, is leaving his post in June 2006. Insiders say this is because of a furious row between himself and Donald Rumsfeld. Rumsfeld wanted the NGA to remain under the direct control of the Pentagon, but Clapper told Congress in 2004 it would not harm the agency's work if it was answerable to powers outside the defence department. He wasn't alone, Michael V. Hayden, then director of the National Security Agency said the same. Rumsfeld wasn't happy and invited them to lunch where he expressed his fears. In 2005 The Office of the Director of National Intelligence was approved and it currently oversees the all 15 US intelligence agencies, more than 80 percent of whose funding comes through the Pentagon. For the record, Hayden is now the second in command to Director of National Intelligence John D. Negroponte.

The National Geospatial-Intelligence Agency, based in Bethesda, collects intelligence from high-powered satellite photos and produces detailed maps for



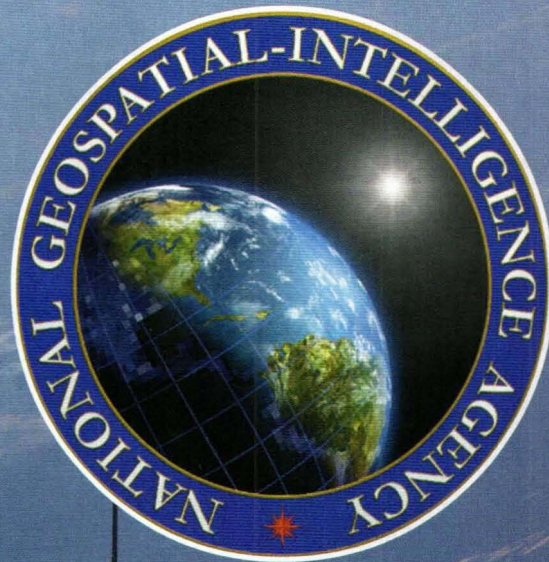
James R. Clapper



John D. Negroponte



Donald Rumsfeld



CORRIDORS OF POWER

INTELLIGENCE IMAGERY

SPYMASTER FEELS THE FORCE

various government departments. It has an annual budget of \$2 billion. The NGA is reportedly the third largest intelligence agency, with about 8,000 staff.

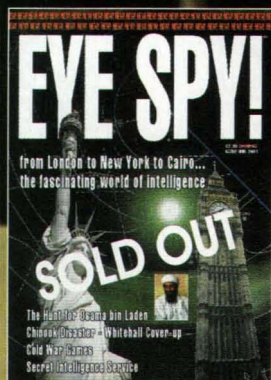
Since 9/11, one of the biggest problems for the NGA is proving it is still a priority industry. America's primary foe - al-Qaida - does not use major weapons systems which can be photographed and analysed by the agency's highly skilled operatives. However, foreseeing this problem, Clapper, 64, widened the work of the NGA to examine intelligence reports from ground-based sources. He played a pivotal role in changing the name of the agency in 2003 from the National Imagery and Mapping Agency to its current one.

Clapper has many friends in the intelligence industry and several have questioned the decision of Mr Rumsfeld. Retired Lt. Gen. Patrick Hughes, former

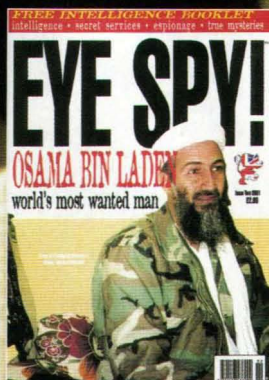
director of the Defense Intelligence Agency, said: "Clapper rescued a floundering agency and completely turned it around. His departure would be our loss; the country's loss."

Dutch Ruppertsberger, who sits on the House Intelligence Committee said: "I have concern about changing leadership [at the NGA] in a difficult time for our country."

Since the United States was attacked, several key intelligence officials have left the CIA and other agencies. Clapper is the latest casualty as Washington continues to shuffle its intelligence pack. His successor, rumoured to be a three-star general, will inherit a controversial satellite programme known as Future Imagery Architecture - a system Negroponte is also trying to overhaul.



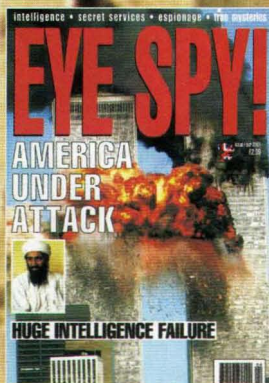
ISSUE 1 REF: ES/01
USA \$7.00 UK £3.50 EUR €4.50



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



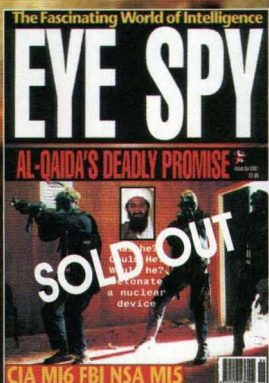
ISSUE 3 REF: ES/03
USA \$7.00 UK £3.50 EUR €4.50



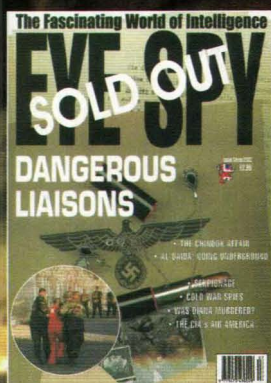
ISSUE 4 REF: ES/04
USA \$7.00 UK £3.50 EUR €4.50



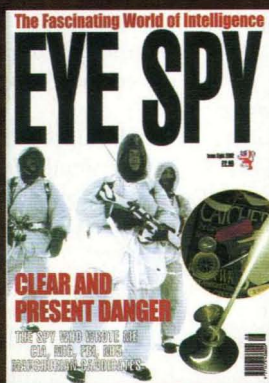
ISSUE 5 REF: ES/05
USA \$7.00 UK £3.50 EUR €4.50



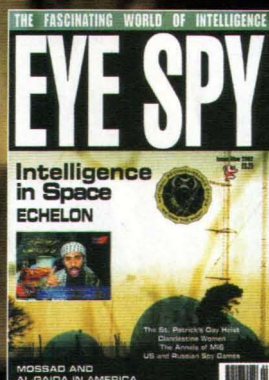
ISSUE 6 REF: ES/06
USA \$7.00 UK £3.50 EUR €4.50



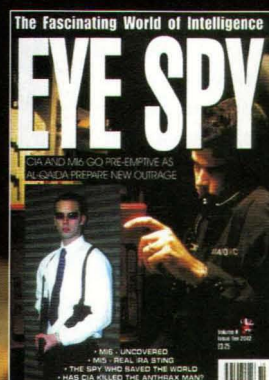
ISSUE 7 REF: ES/07
USA \$7.00 UK £3.50 EUR €4.50



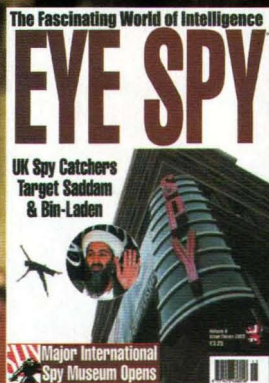
ISSUE 8 REF: ES/08
USA \$7.00 UK £3.50 EUR €4.50



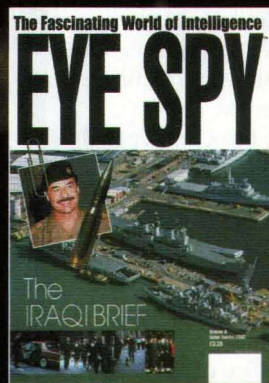
ISSUE 9 REF: ES/09
USA \$7.00 UK £3.50 EUR €4.50



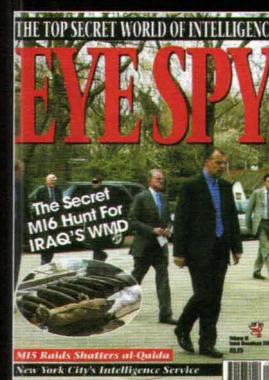
ISSUE 10 REF: ES/10
USA \$7.00 UK £3.50 EUR €4.50



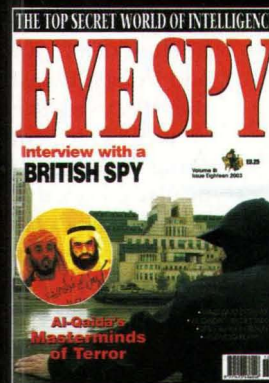
ISSUE 11 REF: ES/11
USA \$7.00 UK £3.50 EUR €4.50



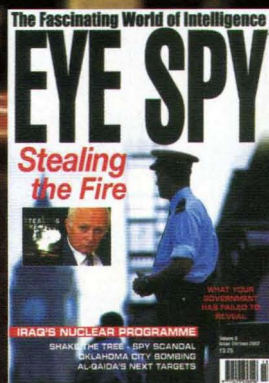
ISSUE 12 REF: ES/12
USA \$7.00 UK £3.50 EUR €4.50



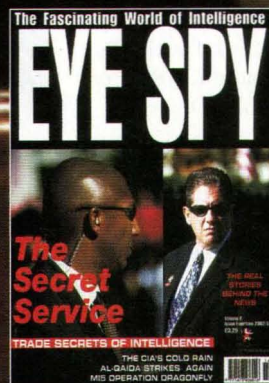
ISSUE 17 REF: ES/17
USA \$7.00 UK £3.50 EUR €4.50



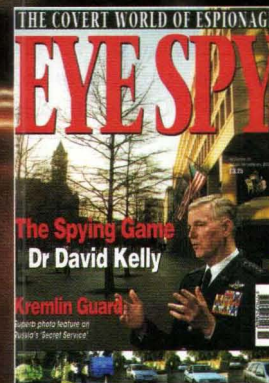
ISSUE 18 REF: ES/18
USA \$7.00 UK £3.50 EUR €4.50



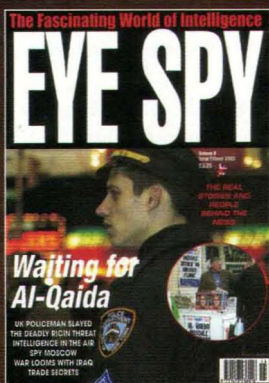
ISSUE 13 REF: ES/13
USA \$7.00 UK £3.50 EUR €4.50



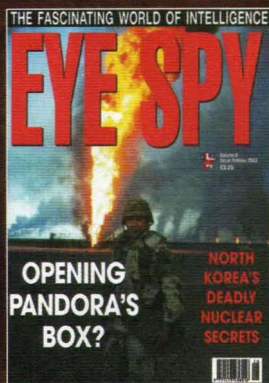
ISSUE 14 REF: ES/14
USA \$7.00 UK £3.50 EUR €4.50



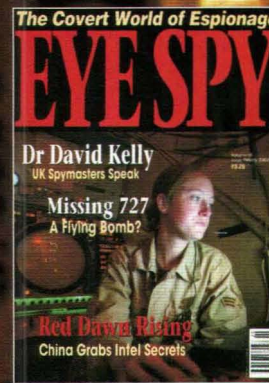
ISSUE 19 REF: ES/19
USA \$7.00 UK £3.50 EUR €4.50



ISSUE 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

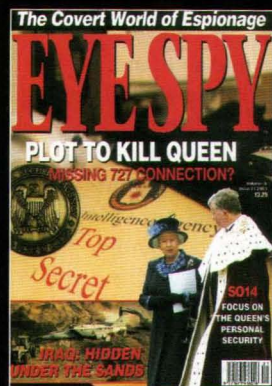


ISSUE 20 REF: ES/20
USA \$7.00 UK £3.50 EUR €4.50

THREE

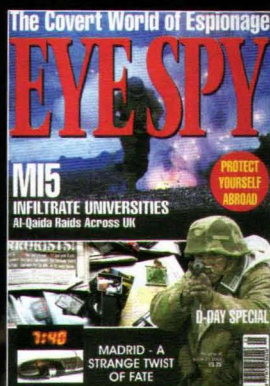
VOLUME FOUR

VOLUME FIVE



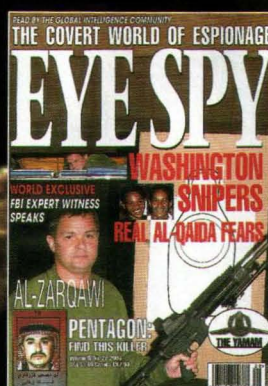
ISSUE 21 REF: ES/21

USA \$7.00 UK £3.50 EUR €4.50



ISSUE 25 REF: ES/25

USA \$7.00 UK £3.50 EUR €4.50



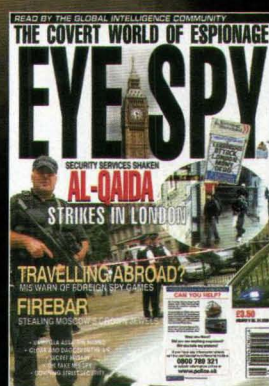
ISSUE 29 REF: ES/29

USA \$7.00 UK £3.50 EUR €4.50



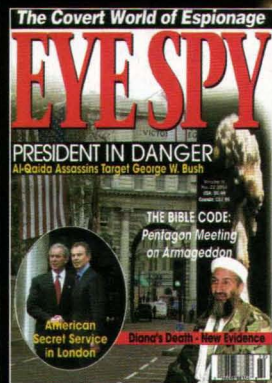
ISSUE 33 REF: ES/33

USA \$7.00 UK £3.50 EUR €4.50



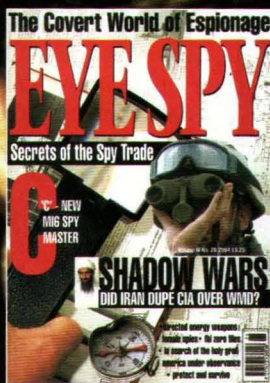
ISSUE 34 REF: ES/34

USA \$7.00 UK £3.50 EUR €4.50



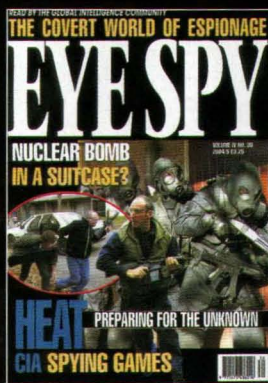
ISSUE 22 REF: ES/22

USA \$7.00 UK £3.50 EUR €4.50



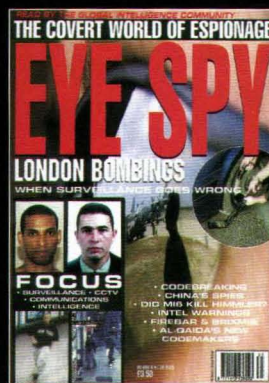
ISSUE 26 REF: ES/26

USA \$7.00 UK £3.50 EUR €4.50



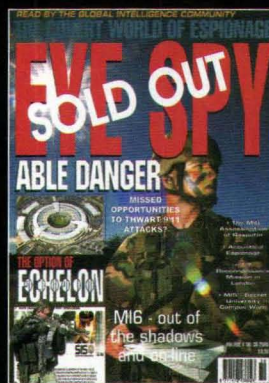
ISSUE 30 REF: ES/30

USA \$7.00 UK £3.50 EUR €4.50



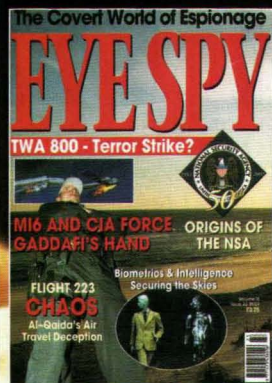
ISSUE 35 REF: ES/35

USA \$7.00 UK £3.50 EUR €4.50



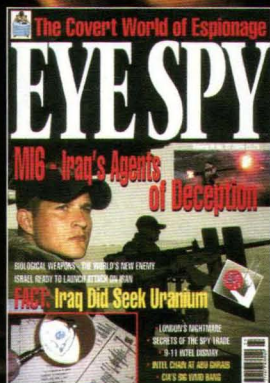
ISSUE 36 REF: ES/36

USA \$7.00 UK £3.50 EUR €4.50



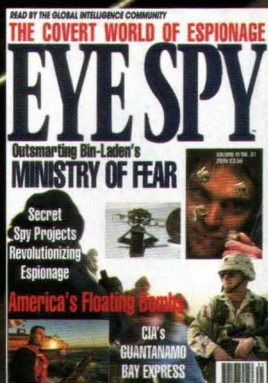
ISSUE 23 REF: ES/23

USA \$7.00 UK £3.50 EUR €4.50



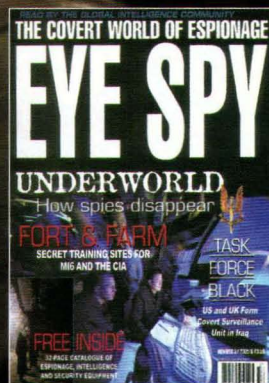
ISSUE 27 REF: ES/27

USA \$7.00 UK £3.50 EUR €4.50



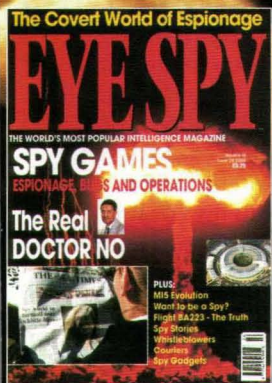
ISSUE 31 REF: ES/31

USA \$7.00 UK £3.50 EUR €4.50



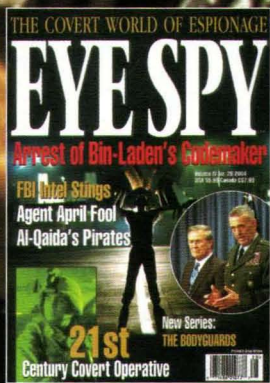
ISSUE 37 REF: ES/37

USA \$7.00 UK £3.50 EUR €4.50



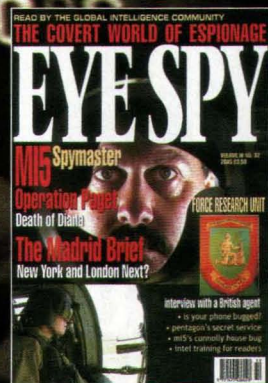
ISSUE 24 REF: ES/24

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

EYE SPY
BACK ISSUES

ORDER FROM UK
OR NEW YORK
(SEE PAGE 82)
OR ON-LINE

www.eyespy.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 world-
wide overview of global
events - your bridge to the
covert world of espionage
and intelligence

Collect copies in
Volumes and save! - see page

M A G A Z I N E B A C K I S S U E S

THREE

VOLUME FOUR

VOLUME FIVE

Eye Spy
PLOT TO KILL QUEEN
MISSING 727 CONNECTION?
Top Secret
5014
FOCUS ON THE QUEEN'S PERSONAL SECURITY
1990: HIDDEN UNDER THE SANDS

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

Eye Spy
PRESIDENT IN DANGER
Al-Qaida Assassins Target George W. Bush
THE BIBLE CODE: Pentagon Meeting on Armageddon
American Secret Service in London
Diana's Death - New Evidence

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

Eye Spy
TWA 800 - Terror Strike?
MI6 AND CIA FORCE GADDAFI'S HAND
ORIGINS OF THE NSA
Biometrics & Intelligence
Securing the Skies
FLIGHT 223
CHAOS
Al-Qaida's Air Travel Deception

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

Eye Spy
SPY GAMES
ESPIONAGE, BUGS AND OPERATIONS
The Real DOCTOR NO
PLUS: Was Evolution Worth It? Is a Spy? Fight SA223 - The Truth
Spy Games
Whistleblowers
Countries
Key Outlets

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

Eye Spy
MI5
INFILTRATE UNIVERSITIES
Al-Qaida Hides Across UK
PROTECT YOURSELF ABROAD
D-DAY SPECIAL
7:40
MADRID - A STRANGE TWIST OF FATE

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

Eye Spy
Secrets of the Spy Trade
NEW MI6 SPY MASTER
SHADOW WARS
DID IRAN OUPPE CIA OVER WAND?
Secrets of the Spy Trade
MI6 - out of the shadows and online

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

Eye Spy
MI6 - Iran's Agents of Deception
Iran Did Seek Uranium
FBI Intel Stings
Agent April Fool
Al-Qaida's Pirates
New Series: THE BODYGUARDS
21st Century Covert Operative

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

Eye Spy
Arrest of Bin-Laden's Godmaker
FBI Intel Stings
Agent April Fool
Al-Qaida's Pirates
New Series: THE BODYGUARDS
21st Century Covert Operative

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

Eye Spy
WASHINGTON SNIPERS
REAL AL QAIDA FEARS
AL-ZARQAWI
PENTAGON: FEAR THIS KILLER
THE MADRID BRIEF
New York and London Next?

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

Eye Spy
NUCLEAR BOMB IN A SUITCASE?
HEAT
CIA SPYING GAMES
PREPARING FOR THE UNKNOWN

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

Eye Spy
Outsourcing Bin-Laden's MINISTRY OF FEAR
Secret Spy Projects
Revolutionizing Espionage
America's Floating Bombs
CIA's GUANTANAMO BAY EXPRESS

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

Eye Spy
MI5 Spymaster
Operation Paget
Death of Diana
The Madrid Brief
New York and London Next?

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

Eye Spy
CIA'S GHOST FLIGHTS
PROTECTING YOUR IDENTITY
MIND READING
THE MADRID BRIEF
New York and London Next?

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

Eye Spy
AL-QAIDA STRIKES IN LONDON
TRAVELLING ABOARD?
FIREBAR
STEALING MOSCOW'S SECRETS

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

Eye Spy
LONDON BOMBINGS
FOCUS
COCKSMAN'S CHINA'S SPY
DID MI6 KILL HERRING?
FIREBAR'S BRITAIN
AL-QAIDA'S BOMB COCKSMAN'S

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

Eye Spy
ABLE DANGER
MISSING OPPORTUNITIES TO THWART 9/11 ATTACKS
THE OPTION OF ECKELON
MI6 - out of the shadows and online

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

Eye Spy
UNDERWORLD
How spies disappear
FORT & FARM
SECRET TRAINING SITES FOR MI6 AND THE CIA
TASK FORCE BLACK
US and UK Form Covert Surveillance Unit on Page

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

**EYE SPY
BACK ISSUES**

ORDER FROM UK
OR NEW YORK
(SEE PAGE 82)
OR ON-LINE

www.eyespymag.com

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

NORTH AMERICAN
READERS
TOLL FREE:
877 309 9243

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

Collect copies in
Volumes and save! - see page



SECRET SIGNALS

**WORLD'S MOST SECRET
INTELLIGENCE AGENCY
EAVESDROPPING
INSIDE UNITED STATES**

Newspapers and television companies in the United States have published reports that America's primary overseas communications' spy agency - the NSA, has intercepted phone calls and e-mail messages from American citizens living on US soil. Under existing legislation that has been deemed "illegal" by some law makers. Unfortunately, the media has not been so transparent in acknowledging that the US-based operation was generated by intelligence picked up outside the country. Eye Spy can reveal that of 30 known 'domestic spy operations' carried out inside the USA, nearly all were activated because US telephone and cellphone information had been discovered on various persons suspected of terrorist links. One intelligence operation helped thwart an attack on the Brooklyn Bridge, and other wire-taps followed after telephone numbers and addresses were 'back-

- NSA 'PLA

tracked' from a number of 9/11 hijackers who resided or stayed in the USA prior to the actual attack. Nevertheless, the very fact that NSA is operational within the USA is regarded as controversial.

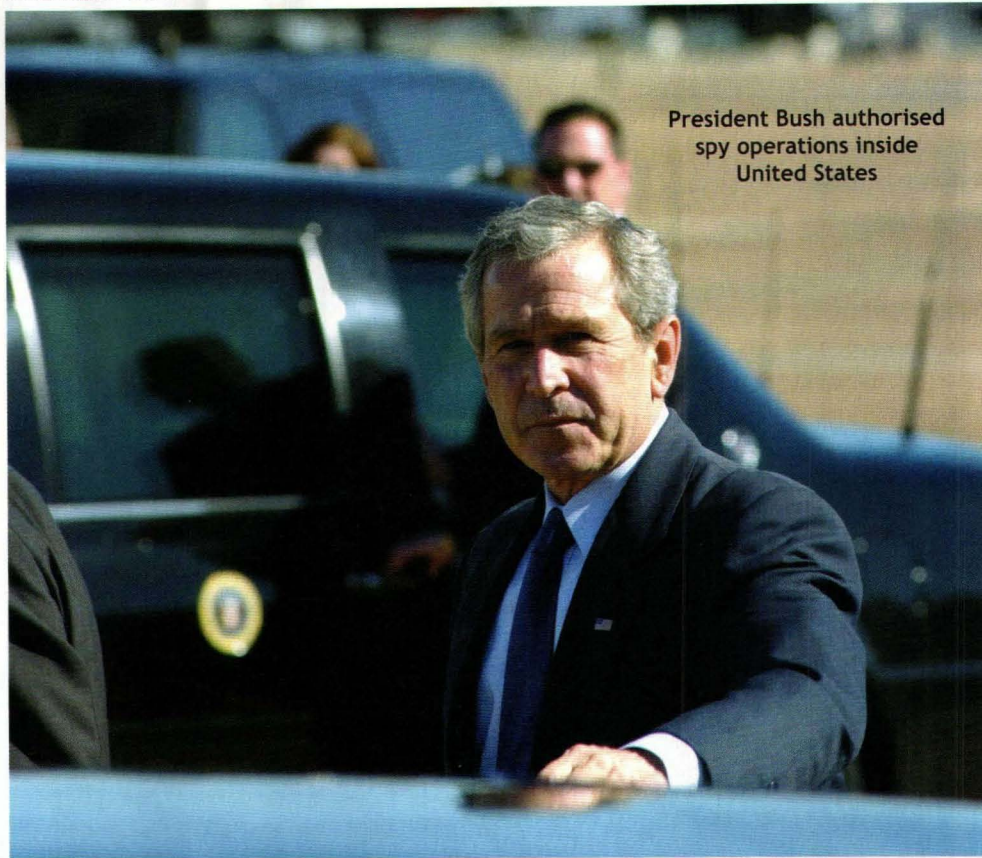
In mid-December, President Bush acknowledged that he was responsible for ordering the NSA to conduct electronic eavesdropping without first obtaining warrants. The president did not provide details on when the highly classified programme began, but did say it would continue because it was "a vital tool in our war against the terrorists." In his weekly address he said his action "was "fully consistent with my constitutional responsibilities and authorities."



His opponents disagreed and voted to block the reauthorisation of America's USA Patriot Act. This law gave the government a green light to expand surveillance operations without a warrant, and was introduced in the aftermath of 9/11.

The NSA has a vast eavesdropping capability and can intercept millions of communications worldwide. However, it is barred from domestic spying, but can apply for a warrant issued with the permission of a special court called the Foreign Intelligence Surveillance Act Court. It appears President Bush bypassed the court and instructed the NSA to proceed with spy operations, using the Patriot Act as a reason for the eavesdropping.

Many intelligence experts believed at least some "internal NSA surveillance" was happening, but for the president to confirm the eavesdropping operation



President Bush authorised spy operations inside United States

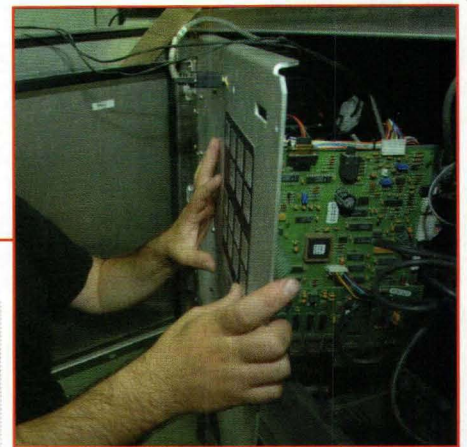
ING AT HOME'



was a surprise. However, efforts are now underway to find the 'mole' who leaked details of the spying to the US media, and in particular, the president's foes.

The intelligence leak is damaging to the NSA, and persons under observance could change their modus operandi, making it virtually impossible to con-

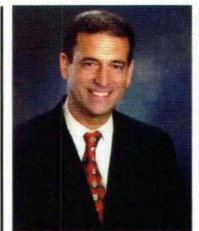
tinue surveillance. "Our enemies have learned information they should not have, and the unauthorised disclosure of this effort damages our national security and puts our citizens at risk" said Mr Bush. "Revealing classified information and details of this secret programme is illegal and alerts our enemies and endangers our country." Mr Bush said



the information had been "improperly provided to news organisations." The president said that his actions were "permissible," but that leaking the revelation to the media was "illegal."

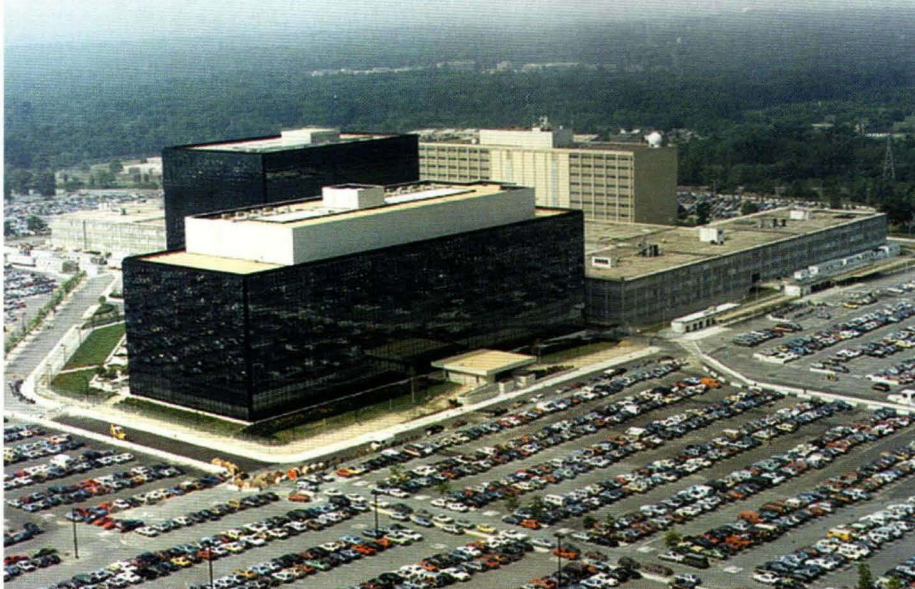
Those who support the action say the NSA effort is crucial to "outing terrorist sleeper cells" in the USA and elsewhere. Sceptics say the White House should have used existing legislation to acquire wiretap warrants.

"He's trying to claim somehow that the authorisation for the Afghanistan attack after 9/11 permitted this, and that's just absurd," Senator Russ Feingold said.



Senator Russ Feingold

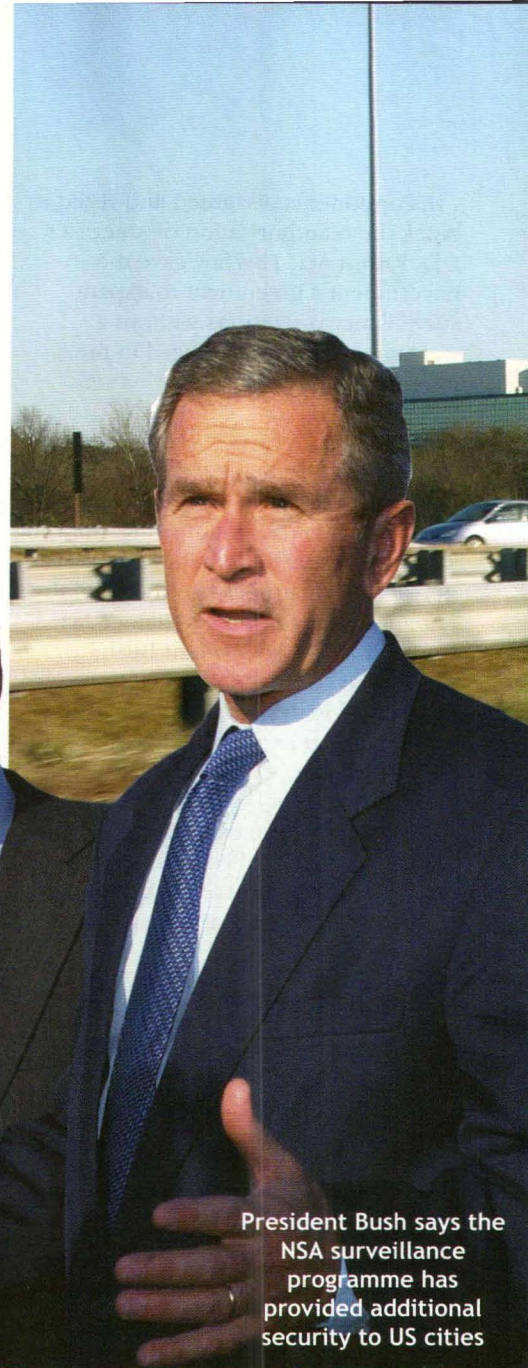
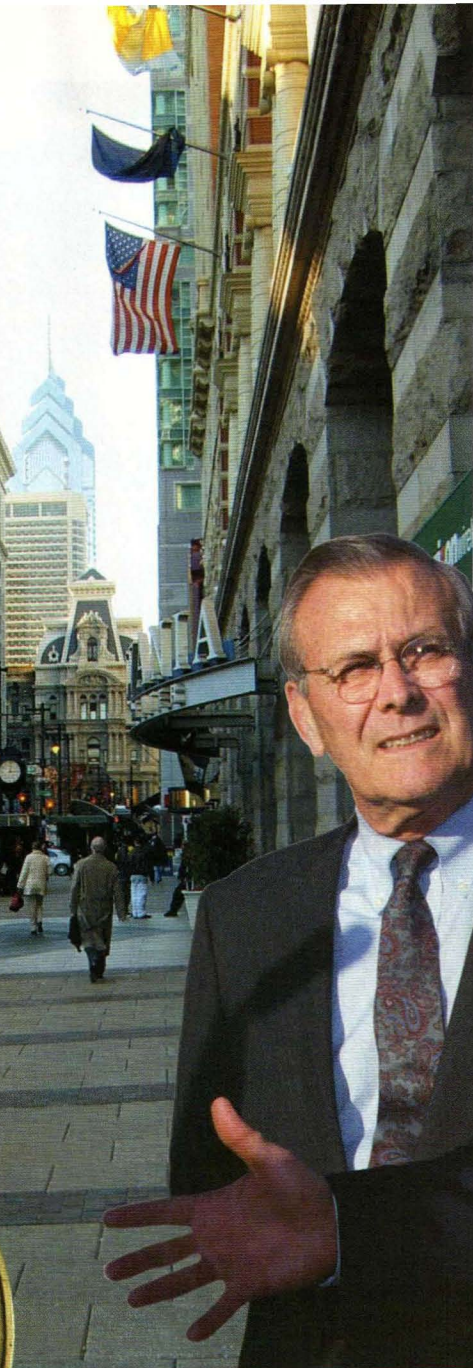
COURTESY: NATIONAL SECURITY AGENCY



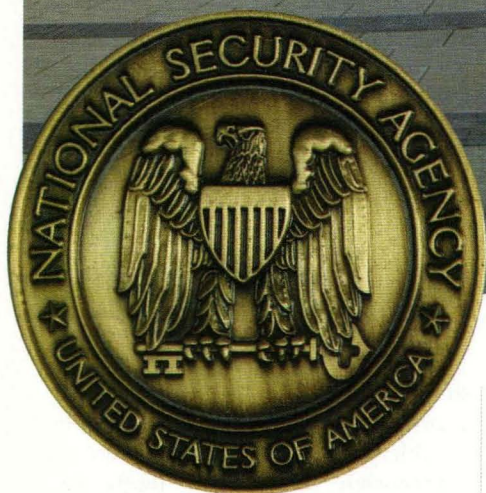
NSA headquarters - Fort Meade



NSA Director
Lieutenant
General Keith
B. Alexander



President Bush says the
NSA surveillance
programme has
provided additional
security to US cities



"There's not a single senator or member of Congress who thought we were authorizing wiretaps. If he needs a wiretap, the authority is already there - the Federal Intelligence Surveillance Act. They can ask for a warrant to do that, and even if there's an emergency situation, they can go for 72 hours as long as they give notice at the end of 72 hours." Those working in the surveillance industry say that some surveillance operations can never be measured in hours. "Eavesdropping on a certain line or cell phone is far more complex than it appears," an Eye Spy associate editor said. "Determining who is on the other end of the line is sometimes impossible. Communications are now being made

using codewords and pictures. It would make sense to use the NSA in certain cases, not least because of its experience in codebreaking and other areas.

TOTAL ELECTRONIC SURVEILLANCE

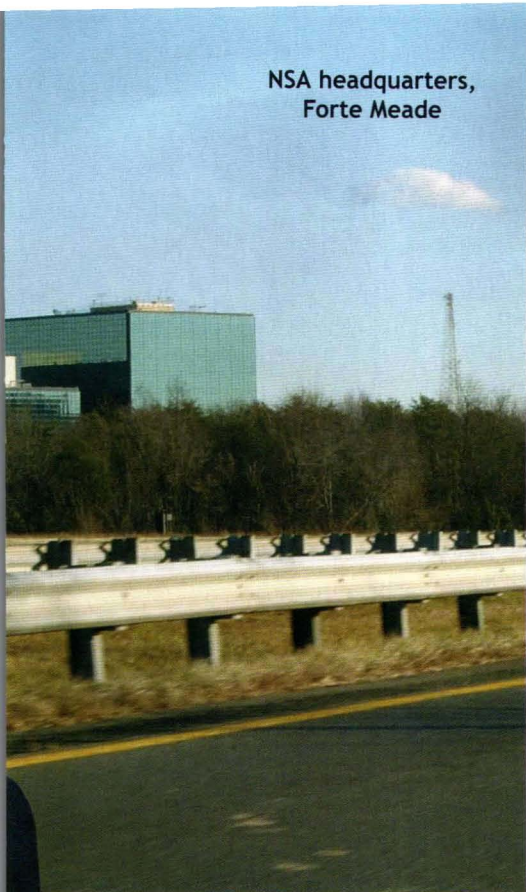
"The NSA is by far the most suitable of all intelligence bodies to acquire electronically data," another US intelligence source told Eye Spy. "Few politicians understand the complex methods required - firstly to obtain the information, and in some cases decode the real meaning of the message or data." Eye Spy has also learned that some intelligence gleaned from persons residing in the United States resulted in further global investigations. "In some cases it's simply not practical to continually pass on surveillance from one group to another, especially if the person under observance is travelling from one

continent to another. This makes the NSA a prime candidate for 'total surveillance', even if it means listening on US dedicated phone lines."

The September 11 Commission discovered two of the 9/11 hijackers on US soil were in contact with al-Qaida cells abroad. "We did not know who they were until it was too late," a senior intelligence figure said. It is understood the NSA and other agencies have approximately 7,000 suspects under surveillance outside the United States. A number of these suspects regularly telephone numbers in the USA and it is these telephones that are being monitored.

For his part, President Bush is adamant the electronic surveillance was essential to security: "This is a different era, a different war. People are changing phone

NSA headquarters,
Forte Meade



numbers and phone calls, and they're moving quick. And we've got to be able to detect and prevent. I keep saying that, but this... requires quick action. I want senators from New York or Los Angeles or Las Vegas to go home and explain why these cities are safer. It is inexcusable to

say, on the one hand, 'connect the dots' and not give us a chance to do so."

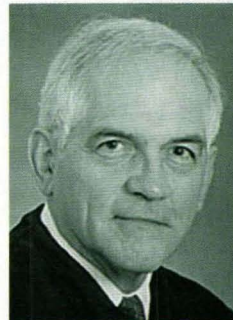
Once the NSA had acquired relevant intelligence, the material is almost certainly passed to the FBI and CIA. President Bush did not comment on this aspect of the eavesdropping. Similarly, it has not known if any 'sister' organisation such as GCHQ (located in England), participated in the spy programme. This is a grey area and one that could have law makers digesting the contents of their law books.

It is believed that the NSA was given "continuation eavesdropping authorisation" 30 times, though it is not known on how many suspects. Some intelligence analysts, however, believe between 500-750 people were placed under surveillance due to electronic intelligence gathered by the NSA. The programme is reviewed every 45 days by the Justice Department and White House.

The White House admission is reminiscent of President Eisenhower's in 1960. He admitted that he authorised U-2 spy flights over the Soviet Union after Francis Gary Powers was shot down on a reconnaissance mission. Such flights over foreign territory were undoubtedly controversial, and probably bordering on illegal.

INTELLIGENCE JUDGE (FISA) RESIGNS

In response to the wiretap revelations, US District Judge James Robertson, an outspoken critic of the president and one of 11 members of the secret Foreign Intelligence Surveillance Court, resigned without providing an explanation.



However, the move is seen as a protest against domestic spying by the NSA. Robertson had privately expressed deep concern that the warrantless surveillance programme was legally questionable and may have tainted the FISA court's work.

Some senior politicians have called for a joint investigation by the Senate judiciary and intelligence panels into the classified programme. However, though the issue is controversial, senior intelligence advisors backed White House assertions that the surveillance is a vital tool in the war against al-Qaida.

THE NSA WHISTLEBLOWER

SOURCE WAS DISMISSED BY NSA IN 2005

It's not the first time anyone with inside knowledge of the mechanisms of intelligence gathering has gone public with information, but Russell Tice, a longtime insider at the NSA, says he gave the *New York Times* details of the secret operations. Furthermore, he says they violated the law.

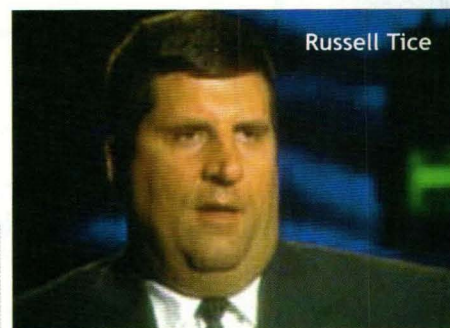
For 20 years Tice listened in to conversations across the globe, but for reasons known only to him, he didn't like turning the machines on to eavesdrop domestic lines.

He told ABC News: "I specialised in what's called special access programmes. We called them 'black world' programmes and operations." After 9/11, Tice says every effort was made to chase the terrorists: "The mentality was we need to get these guys, and we're going to do whatever it takes to get them." Clearly Tice didn't agree with everything at the NSA and is prepared to tell Congress what he knows.

INTERCEPTING CALLS

Many at the NSA feel badly let down by Tice after he exposed some of the technology and analysis conducted by the listening service. He says technology exists to track calls entering the country, leaving the country and those of a domestic nature. For example, calls wend their way through telephone exchanges and can be monitored and tracked. "If you picked the word 'jihad' out of a conversation," Tice said, "the technology exists that you focus in on that conversation, and you pull it out of the system for processing."

Tice said that analysts develop graphs that resemble spiderwebs linking one suspect's phone number to hundreds or even thousands more. He then went on to say that he disagreed with the NSA intercepts without proper warrants and that if the agency used its full huge capacity to intercept calls, millions of Americans would be vulnerable. "That would mean for most Americans that if they con-



Russell Tice

COURTESY: ABC NEWS

ducted, or you know, placed an overseas communication, more than likely they were sucked into that vacuum," Tice said.

Tice dismissed charges that he was a whistleblower. "As far as I'm concerned, as long as I don't say anything that's classified, I'm not worried," he said. "We need to clean up the intelligence community. We've had abuses, and they need to be addressed."

Perhaps his bitterness can be put down to the fact that in May 2005, the NSA removed his security clearance, saying it had psychological concerns. He was later sacked. When asked about his dismissal, Tice told ABC: "That's bunk ... it's the way the NSA deals with troublemakers and whistleblowers."

SPIES



Margaret Lourdes is an attorney in Detroit and a faculty member of Cleary University in Ann Arbor Michigan, where she teaches graduate level law courses

SILENT
TROOPS IN
THE FIELD -
SUPPORTING
THEM
THROUGH AN
AMENDMENT
TO THE LAW

OR SILENT WA

The public naming of any serving intelligence officer or agent is considered controversial, in some cases it is illegal. **MARGARET A. LOURDES** examines the implications surrounding the 'outing' of Valerie Plame, a CIA officer of 20 years, and asks what price security against freedom of speech. Was it really necessary?

Soon after the Twin Towers disappeared into ashes, President George W. Bush informed the American people that they were fighting a new and different kind of enemy.

Bush underscored the crucial need to support and utilize our intelligences services, if America was to have any hope of prevailing against terrorism.¹ The US government proceeded with an enormous overhaul of the intelligence community. Efforts began to erode "the wall" which traditionally existed between intelligence gathering services and law enforcement.

Ironically, shortly after the attacks on New York and Washington DC, a governmental official leaked the name of CIA operative Valerie Plame to columnist Bob

Novak. During Plame's twenty year career at the CIA, she had worked clandestinely overseas in a non-official capacity (NOC). NOC positions mean an agent conducts overseas missions without the diplomatic protections of the United States Government, which can result in execution if the operative is captured.² At the time of the name disclosure, she was working within the United States, but continued to maintain false identities and undercover status. The CIA had specifically asked Novak not to reveal Plame's identity at the time he inquired about her position with the Agency.³ Notwithstanding, in 2003 Novak published her name.

In 1982, President Ronald Reagan signed the Intelligence Identities Protection Act into law.⁴ Opponents of the act believe it

'chills' free speech rights, which are such a fundamental cornerstone of American law and tradition. Indeed, when the Intelligence Identities Protections Act was created free speech was of utmost concern. Congressional conference accounts are replete with references to



Valerie Plame and husband Joseph Wilson

COURTESY: VANITY FAIR

the 1st Amendment and the importance of meeting its muster.⁵

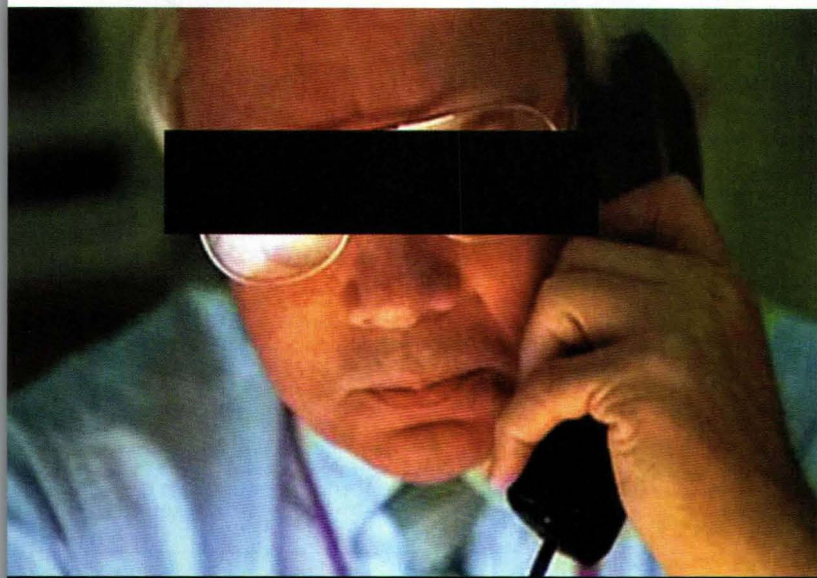
The Act covers two different classes of persons. Those who have access to classified information and those who do not have access to classified information. Section 601(c) of the Act precludes those who do not have access to classified information from committing "pattern" name disclosures. Because this section

ports or the number and location of troops" may be prevented.⁸

The War on Terrorism will be ongoing and turns on the success and failures of the intelligence communities. It stands to reason, therefore, that covert agents are analogous to troops in the field.

Moreover, in light of 11 September and the numerous other attacks worldwide since 2001, free speech that serves no legitimate purpose and may, in fact, undermine security must reasonably be viewed under a heightened level of scrutiny.

Although the Act was originally drafted to proscribe only "pattern disclosures," by



RRRIORS?

can silence the voices of everyone, not just those who have consciously vowed to keep confidences, opponents argue it infringes on the constitutional right to free speech.⁶

The elements of Section 601(c) state anyone making the disclosures must firstly be aware that the agent is covert and, secondly, must be aware that disclosing the name may compromise national intelligence gathering work. These requirements obviously target reckless exposures, not protected, free speech. Idle conversations, rumours and hearsay chat among citizens are not covered.

Indeed, precedent renders it extraordinarily difficult for the government to restrain in advance the content of one's speech.⁷ However, in times of war, the rules relating to speech change. The well-settled "Troopship" exception states: "[In times of war] actual obstruction to [the government's] recruiting service or the publication of the sailing dates of trans-

persons outside of the classified loop, times have changed and so too should the Act. As we know, the Act currently does not cover a single disclosure such as the one made by Bob Novak. Nevertheless, it must not be ignored that Novak exposed a covert agent with impunity, during a time when the world is fiercely fighting terrorism.

Realistically, a pattern of disclosures may not be required to lead to another



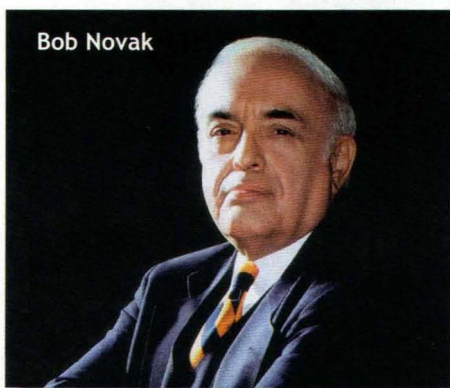
Identifying agents could affect on-going operations

terrorist attack. Consequently, the language of Subsection 601(c) should be bolstered. Any time anyone is in the possession of a covert agent's name, publishing it in a media forum has no compelling purpose. Opponents allege there may be times when it would warrant an agent's name being disclosed. Novak would argue this was the case with the Valerie Plame occurrence. Plame's husband, Joe Wilson, was sent to Africa, allegedly at the behest of the CIA prior to the Iraq conflict. Based on his trip, he returned with criticisms of the Bush Administration's claims for war against Iraq.⁹ Was the fact that Wilson was married to Plame a sound predicate to compromise secret projects Plame was involved in for the CIA?

Changes to the Act could easily make proper exceptions to safeguard against legitimate exposures. For instance, people with information relating to improper acts may always report alleged improprieties to those with authority to weed out and punish wrongdoers. Furthermore, the story of any alleged misbehaviour could be reported by the media, simply with the caveat of withholding the actual name of covert agents. Reporters, such as Judith Miller of the *New York Times*, vehemently protect the identity of "confidential sources" without any fear that anonymity will diminish the credibility of a story.¹⁰ Miller spent 12 weeks in jail as a result of a federal contempt of court charge, after refusing to divulge information relating to the Plame leak.¹¹ It is hypocritical to hold a "source" that illegally leaks classified information to a higher level of protection than a patriot in the clandestine service.

The Act is crucial for protecting the welfare of individual agents; these are the silent troops in the field. Furthermore, the danger of "naming names" does not stop with compromising the agent alone. It has the potential of reaching and injuring every action and person with which the agent has ever been involved while under working undercover. ➤

Bob Novak

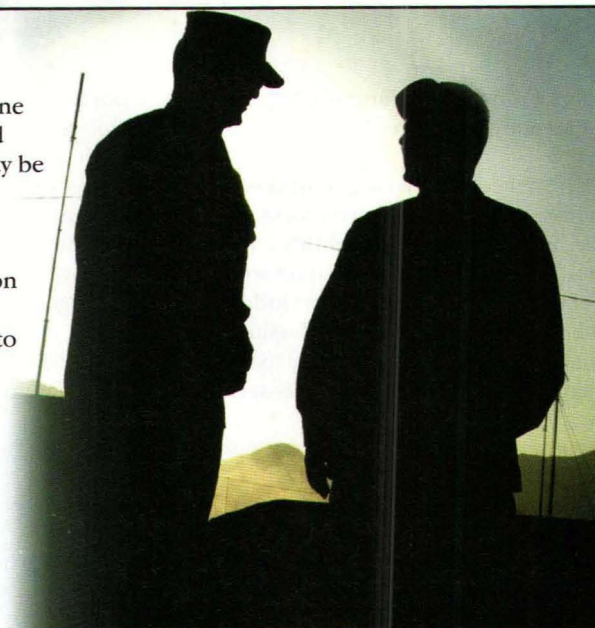


To completely safeguard an overly burdensome restraint on speech, the Act could be amended to create a "rebuttable presumption" in the event "someone without access to classified information publishes the name of a covert agent in a media forum." A rebuttable presumption is: "An ordinary presumption which must, as a matter of law, be made once certain facts have been proved... and which may be rebutted or overcome through the introduction of contrary evidence."¹²

Obviously, at the time the agent's cover is blown, the projects connected to the outed agent will be compromised to some certain degree. Therefore, it is sensible to begin an analysis of a disclosure with the notion no legitimate purposes exists for it. If the project is one of preventing a dirty bomb from entering central London or Los Angeles, the idea of protecting the speaker becomes outrageous. Even so, a presumption could be rebutted, giving someone like Novak the chance to argue why publishing the name of an agent was legitimate.

The American judiciary has long interpreted the constitution with wisdom and reasonable expectations. One cannot

defame another's character; one cannot yell "fire" in a crowded theatre and certain speech may be limited in times of war or for national security. Those who would wish apply the actual, literal words of the constitution to a current or amended reading of Section 601(c) fail to recognise a fact we cannot afford to ignore in a post 9/11 environment. That being, a constitution, which lives and breathes, may be the key to keeping nations living and breathing as the world faces the first great war of 21st Century.



NOTES AND REFERENCES

- 1 7 October 2001, Indianapolis Star, *Bush Addresses the Nation*, (excerpts from Bush speech of 07/10/01 addressing the nation).
- 2 2005 Wikipedia, *Plame Affair* Retrieved from http://en.wikipedia.org/wiki/Plame_affair
- 3 Robert Zelnick *Essay on Source Confidentiality: Journalists & Confidential Sources*, 19 Notre Dame Journal of Law & Ethics (2005).
- 4 50 U.S.C 421-426
- 5 Supra, note 6.
- 6 Lawrence P. Gottesman, *The Intelligence Identities Protection Act of 1982: An Assessment of the Constitutionality of Section 601(c)*, 49 Brooklyn L. Rev., 479

- (1983); Susan D. Charke, *The Constitutionality Of The Intelligence Identities Protection Act*, 83 Columbia L. Rev. 727 (1983)
- 7 Eunice Eun, *Journalists Caught in the Crossfire; Robert Novak, The First Amendment and Journalists Duty of Confidentiality*, 42 Am. Crim. L. Rev. 1073 (2005)
- 8 Near verses. Minnesota, 283 U.S. 697 (1931).
- 9 Supra, note 3.
- 10 Supra, note 9.
- 11 28 October 2005, CNN.Com, *Jailed Reporter Reaches Deal in CIA Leak Probe*, Retrieved from <http://www.cnn.com/2005/POLITICS/09/30/cia.leak/>.
- 12 Steven H. Gifs (1991) *Barrons Law Dictionary*, 3rd Edition, Barrons Educational Series Inc.

INTERNATIONAL CONFERENCE

Post-war intelligence, intelligence after 9/11, the future of intelligence

Conference at Christ Church,
University of Oxford 2-8 September 2006

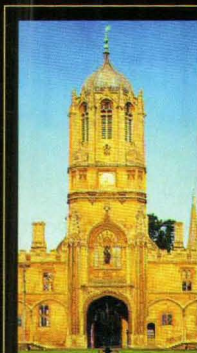
The conference brings together authors, experts and intelligence practioners of international standing and examines the evolution of intelligence, espionage and deception across more than half a century since the end of World War II

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

Speakers include: Professor Richard Aldrich, Chapman Pincher, Professor Christopher Bellamay, Dr David Khan, Nigel West, Bill Duff, Dr Stevey Gibson, Dr Michael Goodman, Mark Seaman, Major R.A.M. Seegar, Dr Stephen J Weiss, Amir Taheri, Baroness Daphne Park... Full speaker biography
www.eyespymag.com



The Conference is organised by Christ Church, a founder member of the Oxford Consortium and an Investor in People organisation

Spies, Lies & Intelligence



Dr. Philip H.J. Davies

WHAT WENT WRONG WITH MI6 ON IRAQ

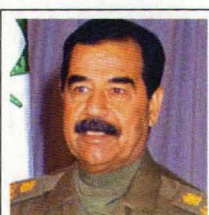
It is now more or less accepted that the intelligence on Iraqi weapons of mass destruction that lay, at least in part, behind the case to go to war in 2003 was wrong. An important factor in that failure was the serious lack of raw intelligence available to the agencies of almost all the major intelligence powers after UN inspectors were withdrawn in 1998. Intelligence on clandestine weapons development programmes has always been a difficult area and prone to error, from British overestimates of German strength in the late 1930s to similar exaggerations of Soviet chemical and biological warfare programmes in the 1980s. Raw intelligence is hard to come by because of the adversary's efforts at denial and deception, and estimates hard to make because guesses about capability become shaped by analysts' perceptions of intentions. ➤

Intelligence and the Missing Munitions





"Maybe over there?" It was clear within a few months that MI6 and CIA intelligence on Iraq's WMD was not accurate



Saddam Hussein's security services made it almost impossible for MI6 to operate agents in reasonable numbers

Against covert weapons programmes, human sources are generally the most useful secret intelligence. Imagery from satellites and 'air breathing sources' (aircraft and land-based photography) is purely circumstantial, and there are often very few telecommunications

signals to intercept because of the enemy's reliance on couriers and shielded landlines. What one needs, therefore, is the traditional two-legged spy walking the corridors of power.

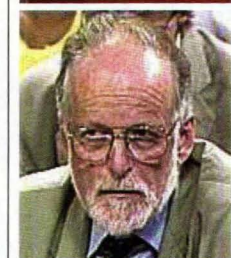
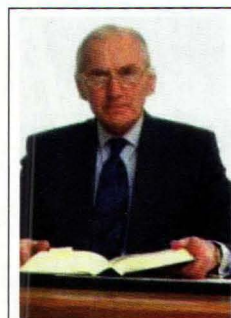
On Iraq, the American intelligence community relied on external evidence from imagery, and a vanishingly small assortment of defectors and émigré sources who had agendas of their own.

With so little technical information available, the British government was forced to rely chiefly on the agents the Secret Intelligence Service (SIS, aka MI6) could recruit in one of the hardest target police states in the world. SIS managed to recruit six sources inside Saddam Hussein's Iraq and run them sometimes for several years under the noses of the Iraqi security services, the Amn-al-Amn and the Mukhabarat. And if Britain only had six spies in Iraq, it was still six more than our larger, richer, better-equipped ally. With those sources, therefore, the problem for Britain is actually how the UK's national analytical body, the Joint Intelligence Committee still got the intelligence picture as wrong as it did.

SIS' SIX SOURCES

A conventional wisdom has evolved since the invasion of Iraq and the subsequent reviews of intelligence in Britain, the United States and Australia, that the raw intelligence in hand was completely

inadequate or misleading. A close examination of the information made available by the British inquiries - by the Intelligence and Security Committee, Lord Hutton and Lord Butler - shows clearly that this is not really the case. Rather, it was the handling of those sources, the failure to effectively separate better quality material from poorer, and the overconfident use of the weaker reporting in JIC assessments, that contributed to the raw intelligence failings on Iraq.



Lord Hutton (top) led an inquiry into the suicide of British weapons expert David Kelly, who was caught up in a vicious dispute over Iraq's WMD

Prior to the invasion, SIS had six sources inside Iraq, two of whom were recruited in between 2001 and 2002, and two more of whom were recruited within the last few months before the invasion. It is important to understand that while SIS may have had six distinct sources or 'lines of reporting' inside Iraq, this is not necessarily a direct indication of exactly how many agents they had in Iraq. At least some of these sources were reporting to their SIS controllers via relatively long '**reporting chains**'. A reporting chain is a series of intermediaries or '**cut-outs**' who pass information from a source to the case officer and instructions back. They provide a protective distance between the human source and intelligence officer should either be under close surveillance from hostile counter-intelligence forces. As a result, while SIS evidently had six independent sources of information, there appears to have been an unknown number of supporting agents working for the Secret Service as cut-outs and couriers for those sources.

Four SIS sources are believed to have reported accurately throughout their tenure as agents on matters of policy and strategy not concerned with WMD. This is a vital point to keep in mind: except on the question of non-conventional weapons, in other words, political, economic and conventional military matters, most of SIS' sources were entirely sound. Because of the urgency of the WMD in the British domestic political arena, SIS

UN inspectors at work in central Iraq 1991



An UNSCOM inspector measures the volume of nerve agent in a container



A bulldozer crushes bodies of 500 kg bombs designed for use as chemical weapons



Declared mustard gas filled bombs



UN inspectors examine shells

controllers tasked the four genuinely reliable agents on that issue even though none of them occupied key positions of access to any Iraqi WMD programme.

As a result, two of the four good sources reported 'less alarmingly' than the others, while the other two turned to hearsay information from amongst their peer groups. One reported simply that it was the common belief in his circle that Iraq had WMDs of some sort, while another turned to an Iraqi official who passed his information to SIS via the established agent. The new sub-agent or 'sub-source' was known by the network's SIS handlers to have sympathy and affiliation with the dissident émigré movement. As a result, the reporting from that sub-agent was passed on to consumers with a warning that the source was known to have a particular agenda in reporting to SIS and this should be taken into account when factoring his information into the assessment process. In the event, that information proved inaccurate and the line of reporting was withdrawn after the war.

The other discredited last-minute source was recruited at roughly the time that the JIC was drafting the so-called *September Dossier*. The September Dossier was the document prepared at the request of the government to make

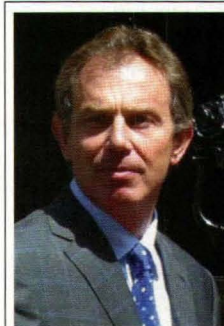
The case for believing Iraq had WMDs. It was based extensively on material also prepared in parallel for a JIC Assessment on Iraqi WMD. When analysts at the Defence Intelligence Staff expressed concerns about the strength of wording in the Dossier's judgements, it was this latter-day source that was invoked to silence their doubts. They were not permitted to inspect the new agent's



product because it was a new source 'on trial', and agents are accepted to be at their most vulnerable when newly recruited. Like the other last minute source, this agent's information has since been discredited and it was subsequently acknowledged that had the DIS analysts had access to the product the fraud might well have been discovered. There remains, in some quarters, a suspicion that this source may have been an Iraqi deception agent, but no definitive

evidence has been found on this one way or the other.

It is also significant to note that the notorious '45 minute report' that figured so centrally in the Dossier was repudiated after the war by the source who was supposed to have provided it. That source was one of those considered generally reliable, and the false claim (plucked out of a Soviet-era military manual) had been introduced into the line of reporting by one of the intervening cut-outs in that agent's reporting chain. Unfortunately, even though the DIS analysts were permitted to see this report, they failed at the time to recognise it for what it was. Human error notwithstanding, this deception could and should have been detected by the available procedures. Indeed, this is true of almost all of the faulty reporting on Iraq. It should have been detected by the existing validation system at SIS headquarters, DIS analysts and the



Prime Minister Tony Blair's comments that Iraqi warheads could be launched in 45 minutes were controversial

LAW ENFORCEMENT PICTURE LIBRARY/STEVE MCMAHON

Assessments Staff when drafting the JIC's reports. The real question since Iraq is why it was not.

REQUIREMENTS AND VALIDATION

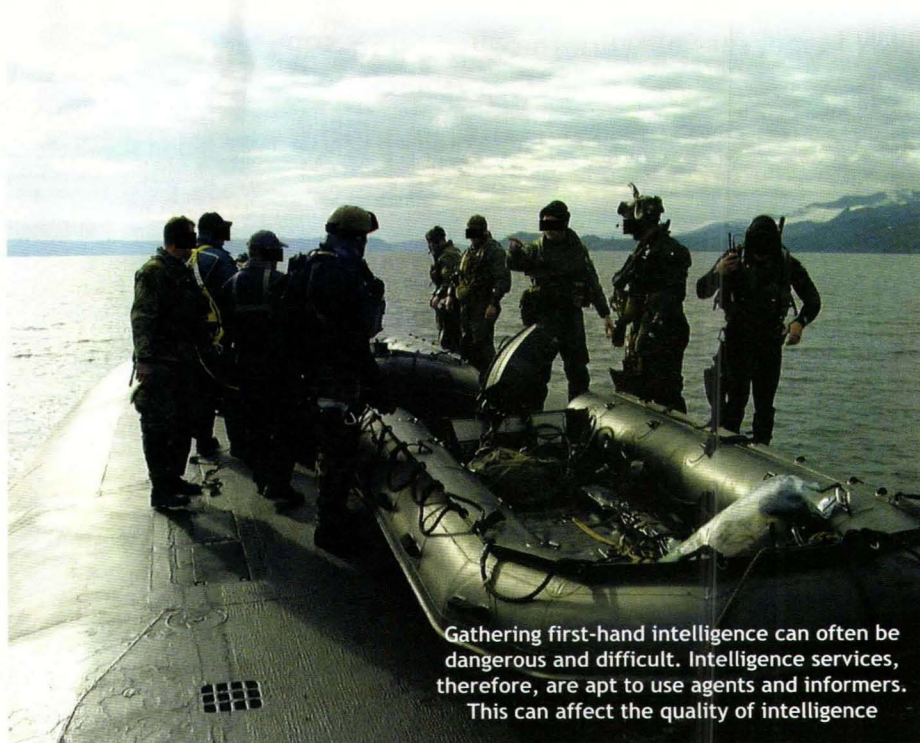
We can see, therefore, that the real problem with SIS reporting was not that its sources were uniformly poor. Rather, there was a systematic failure to adequately separate the good reporting from the bad. This allowed dubious information to be factored into the JIC assessment and, as Lord Butler put it, given greater weight than it could bear.

Indeed, all human intelligence is a mixture of good and bad. Even vital and highly productive sources of the first water require a cautious and exacting use of their information to separate *wheat from chaff*. A classic example is Oleg Penkovsky (see below), an agent for SIS and CIA in Soviet military intelligence in the early 1960s. Penkovsky provided literally thousands of photographed military documents to his British and American controllers. These included the Red Army rocketry manuals that allowed American analysts to identify Soviet medium- and intermediate-range ballistic missile site in Cuba from U2 photographs in October 1962. Penkovsky's reporting also included a considerable volume of personal reporting on political aims and intentions within the Soviet government.

This latter product was so subjective and idiosyncratic that it had to be disseminated under completely different set of 'serials' or lines of reporting, under two different codenames. In America these were IRONBARK for his technical information and CHICKADEE for his political opinions (in the UK the codenames RUPEE and ARNICA were used).

As a result, even the best agent's information needs to be cautiously evaluated and checked for reliability or validated.

Gathering first-hand intelligence can often be dangerous and difficult. Intelligence services, therefore, are apt to use agents and informers. This can affect the quality of intelligence



THE ART OF ESPIONAGE

OLEG PENKOVSKY - SOVIET DOUBLE AGENT

Oleg Penkovsky went from a Russian World War II military hero, to becoming America's best human intelligence asset in the Soviet Union. He believed that Nikita Khrushchev's leadership was taking the Soviet

Union onto the path of destruction. Penkovsky was the highest level Soviet officer to ever spy for the United States or British Intelligence. The Penkovsky case is considered to have been the most successful Cold

War espionage operation. Penkovsky was observed by KGB agents after a meeting with a British intelligence contact, which led to his arrest and execution.

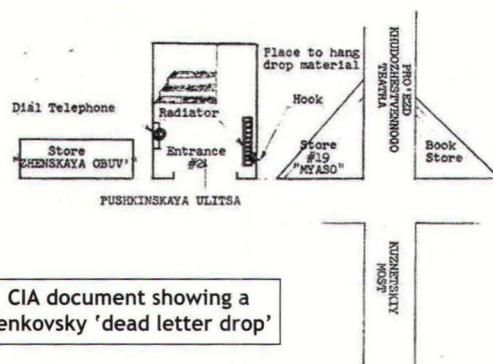
The recruitment of a well-placed spy, in this case a high-ranking Soviet military intelligence officer, lessened the tensions of the Cold War by providing information on the intentions, strength, and technological advancement of the Soviet Union. At the same time, the enormous risks for the spy himself became evident in the fate of Penkovsky, shot as a traitor by the Soviets in 1963 for spying for the

United States and United Kingdom.

Penkovsky allowed the administrations of President Eisenhower and President Kennedy to bypass the bluster and rhetoric of Nikita Khrushchev, and to know the true facts concerning Soviet military prepared-

ness. Penkovsky's acts of espionage were able to define for the United States the limitations of Soviet power. Through Penkovsky, the United States learned of the number of nuclear missiles the Soviets held and the problems with their guidance systems. During the Cuban Missile

PLAN (DIAGRAM) OF DEAD DROP SITE AND ITS LOCATION



product and then passing it to consumers with some kind of grading for its reliability so that analysts and decision-makers can then decide how to factor the information into their judgements, beliefs and decisions.

Lord Butler noted in his review that the validation part of SIS had been so diminished during the budget cuts of the 1990s that it was not equal to the volume and urgency of the demands laid on SIS after 9/11 and before the invasion of Iraq. What Lord Butler did not acknowledge, however, was that the agency's validation

By the time the Cold War ended and the peace dividend axe came down on the British intelligence budget, Requirements was already probably an accident waiting to happen...

organisation, known as its 'Requirements side' had been getting steadily weaker and weaker since the early 1970s. During each round of belt-tightening the agency has had to endure since the 1960s, Requirements was cut back further and further. By the time the Cold War ended and the peace dividend axe came down on the British intelligence budget, Requirements was already probably an accident waiting to happen.

The Requirements 'side' of SIS was originally a number of 'consumer liaison sections' attached from the agency's major consumers - the War Office, Admiralty, Foreign Office, Royal Air Force and later others - to its headquarters after the First World War. In fact, SIS became known as 'MI6' because this was the Military Intelligence designation of the War Office consumer liaison section during the Second World War. When the armed forces were amalgamated under the Ministry of Defence in 1964, that liaison section became Defence Intelligence 6, or DI6, which is why one occasionally sees SIS referred to that way as well.

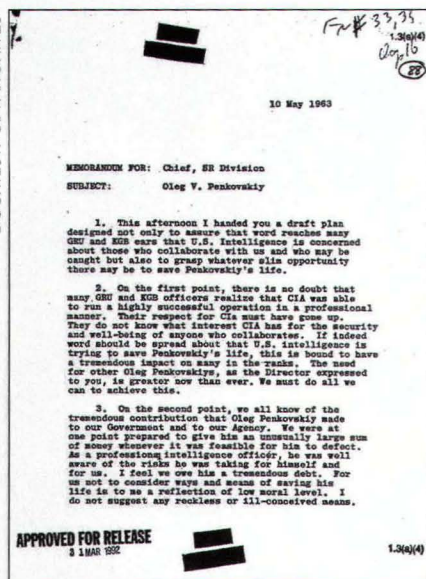
During the 1945-46 post-war reorganisation, these sections were grouped together in a central and influential Directorate of Requirements whose head, D/R, sat on the Board of Directors alongside the head of operations, or

Director of Production (D/P). In 1974, however, when Sir Maurice Oldfield took over as Chief of Service or 'C', Requirements was re-organised along geographical lines. SIS officers were given the task of acting as intermediaries between SIS' operational efforts and the various civilian departments in Whitehall and the JIC who used SIS information in their assessments. At the same time, the representatives of the armed Services were moved from Requirements to a new Secretariat under C as Ministry of Defence Advisors. This meant two things. Firstly, the R Sections were no longer the direct voices of SIS' customers in the British government. Secondly, moving the armed forces representatives to C's Secretariat



Sir Maurice Oldfield

COURTESY: CIA ARCHIVES



Crisis, Penkovsky was able to provide information on how those missiles operated in the field. Soviet GRU (military intelligence) documents provided by Penkovsky, show the friction between the Soviet high command over whether Soviet military strategy should depend on nuclear weapons, or general purpose forces.



Ministry of Defence, Whitehall, London - a primary user of MI6 intelligence

EYE SPY

deprived Director Requirements of the weight of speaking on their behalf on the Board of Directors.

Throughout the 1970s Requirements Directorate found itself politically diminished on the Board. In addition, its staff steadily was cut back as the economic hardships of that decade deepened. In 1979, under Sir Arthur 'Dickie' Franks as C, it was decided Requirements was too small to warrant a full directorate. Requirements and Production were amalgamated under a common Director (D/RP) and Requirements overseen by a Deputy Director (DD/R). DD/R held the same level of seniority as the Area Controllers who directed SIS operations.

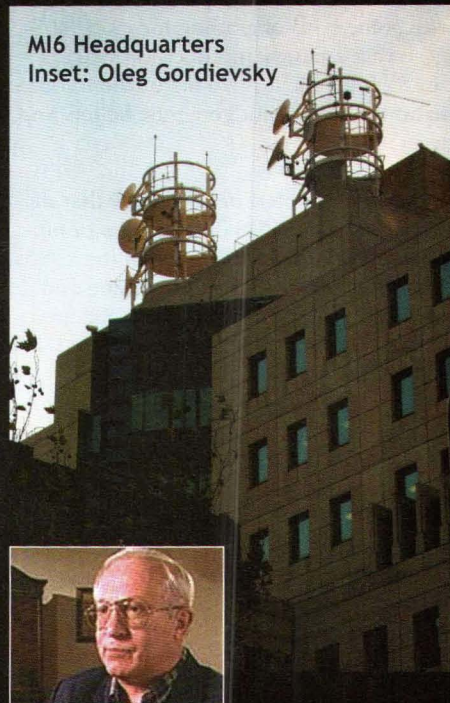
At the same time, SIS began collocating the Requirements Sections with their respective Controllerates (e.g. Requirements/Western Hemisphere with Controller/Western Hemisphere). This closed the gap even further, and in the view of some older officers at the time, risked compromising the objectivity and detachment of the validation process by bringing it too close to the operational officers and their strong personal attachments to their agents or 'Joes'. Unsurprisingly, after a decade of intelligence budget cuts, Britain found herself confronted with the Argentine invasion of the Falklands and

the government of Margaret Thatcher had to rethink its expenditure on intelligence.

Despite increased funding in the 1980s, Requirements remained in its subordinate position on the Board of Directors. In most organisations, management problems tend not to be recognised during the good years, and for SIS the 1980s were very good years indeed. Its stock was high with its consumers in Whitehall, there were substantial intelligence and counter-intelligence successes such as the defections of Oleg Gordievsky and Vladimir Kuzichkin, and the recruitment of the son of a senior Politburo member in the heart of the USSR.

But if the second half of the 1980s was SIS' seven fat years, after Sir Michael Quinlan's post-Cold War review of intelligence in 1994 came its seven lean years. As part of the 'peace dividend', reductions in defence and security spending began to reach the intelligence community (despite Quinlan's recommendations to the contrary). For SIS, the 'peace dividend' consisted of an overall 25% cutback, part of which was a 40% reduction in senior management. To cut top level salaries, DD/R was abolished and the Requirements sections formally subordinated to the Area Controllers. Quality control was now wholly subordinate to production - a situation unthinkable in private industry, and yet welcomed by many in the service as bringing

MI6 Headquarters
Inset: Oleg Gordievsky



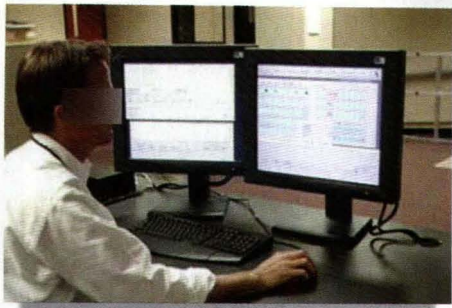
operations even closer to Requirements and the needs of consumers. The Requirements Officers sat on a Requirements Board which had a senior officer as spokesman, but there was no longer any voice for Requirements at the top levels of SIS management.

CRISIS, COLLAPSE AND THE FUTURE

When intelligence demands began to swell after the terrorist attacks on America



"The ability to adequately separate *wheat from chaff* in the reporting SIS receives is vital to the effective exploitation of that information, and essential to ensuring the credibility of SIS with its customers..."



on 9/11, and as attention shifted to Iraq, a system that was already creaking evidently became untenable. Requirements had become a backwater in the agency, staffed in minimal numbers by junior officers and probationers. The tasks laid upon SIS grew rapidly, and although the Government allocated additional funds such things take time to enter the system and make real changes.

During his evidence to Lord Butler, Sir Richard Dearlove, then C, argued that it was not always possible to put one's best officers on attachments to Requirements when the agency was pressed to field as much operational capability as possible. And this is an understandable point of view - almost certainly the same sort of rationale was used for abolishing an

independent Requirements Directorate in 1979. But good validation work has never required large numbers of officers, merely a few experienced and able ones.

The ability to adequately separate *wheat from chaff* in the reporting SIS receives is vital to the effective exploitation of that information, and essential to ensuring the credibility of SIS with its customers. When SIS officials 'at the JIC level' presented marginal intelligence as sound, or refused to give expert analysts access to new information of questionable provenance, there was no senior voice on the SIS Board of Directors to challenge them. It seems likely that when the JIC principals - the Chairman, Intelligence and Security Coordinator and the agency heads - were drafting the September Dossier they became convinced by their own, government-mandated, cherry-picking of the available evidence. And there was no objective, detached voice of validation at the highest level in SIS to question the use of the agency's product to support the judgements it did. In his report, Lord Butler singled the weakness of Requirements out as the main problem with SIS

reporting and the role of that reporting in JIC assessments on Iraq. Nonetheless, he underestimated the depth and duration of that malaise.

Since Lord Butler reported, the Government has sought to assure the public that the SIS is all fixed now, and the agency's credibility should be viewed as restored. According to the Prime Minister's spokesman, an external executive director has been appointed and, more significantly, a new 'head of Requirements' on the same level as the Area Controllers has been established. But all this really does is reinstitute a subordinate Deputy Director of Requirements and return Requirements to its already diminished status before the 'peace dividend' cuts. It is hard to see how effective validation can genuinely be restored within SIS, and its credibility fully regained, until Requirements once again has an independent voice on the Board of Directors at Vauxhall Cross.

© Dr Philip H.J. Davies 2006

Dr. Philip H.J. Davies is the Deputy Director of the Brunel University Centre for Intelligence and Security Studies.



MI6 ATHENS STATION CHIEF NAMED AS GREEK INTEL CONTROVERSY GROWS

A Greek magazine has claimed that a British diplomat, reportedly the head of MI6's station in Athens, was part of an intelligence unit that "abducted Pakistani immigrants" in order to question them about the London terrorist attacks which occurred in July 2005. *Proto Thema* claimed the unit was made up of British and Greek intelligence officers. The magazine also said a [UK] "Government 'D' Notice" had been issued to UK editors to stop the naming of the officials and probable publication of the incident. This is unlikely, though the Defence Advisory Committee can request media organisations not to name MI6 officers - even if their identity has been exposed in foreign publications.

Proto Thema published the supposed identity of a man that appears to match an officer allegedly revealed on the internet in allegations made by the renegade MI6 officer Richard Tomlinson. Given the circumstances of the story, it is likely any named official will be recalled to London.

A Foreign Office spokesman said: "We do not comment on intelligence matters. We are not

confirming or denying this story." An official at the Greek National Information Service said: Our intelligence service never comments on such issues, even when they are non-existent. However, it is our duty to point out that such claims are illegal because they endanger the national security of the country and of allied countries, but also endanger the physical safety of persons who are identified by name."

The magazine feature emerged as several men (testifying before a magistrate) said "Greek and British men forced their way into their homes in four Athens suburbs after the bombings." The men were allegedly taken to various locations and questioned about communications with friends, family and colleagues in the UK. "Two times a policeman hit me while I was on the floor," said Gul Nawaz, a 32-year-old Pakistani who says he has lived in Greece as an immigrant for three years. "I asked him for some water and he punched me hard in the face. Later he kicked me. They confiscated my mobile phone. They wanted to know everything about our friends, relatives and calls to London. They asked us if we had any links to al-Qaida."



Police and Army on the streets of London just minutes after terrorists struck on 7 July 2005

It is also alleged that after questioning, the men were released in Athens city centre in the middle of the night.

In 2004, a number of British intelligence officers operating in the Balkans were moved after their names were published in newspa-

pers. Sources claim their identities were exposed by disgruntled members of local intelligence services. One officer was reportedly the MI6 station chief in Serbia. His photograph appeared on the cover of a Serbian-based magazine.

© LAW ENFORCEMENT PICTURE LIBRARY/STEVE MCMAHUS

Senior intelligence figures have warned politicians in Israel's parliament, the Knesset, that Spring is the 'tipping point' for taking disabling action against Iran's nuclear sites. After that, they warned, Tehran will be less than two years away from producing nuclear weapons.

According to highly-placed military sources, Prime Minister Ariel Sharon received intelligence on several secret Iranian uranium enrichment sites. Before his stroke, he told military planners to prepare for "possible strikes." Sharon said: "Israel - and not only Israel - cannot accept a nuclear Iran. We have the ability to deal with this and we're making all the necessary preparations to be ready for such a situation."

Those "preparations" began over two years ago and involved Israel's powerful air force. Several key sites have been identified that will almost certainly be targeted if diplomatic negotiations between Britain, France, Germany and Iran break down. Indeed, Israeli F-151



fighter jets have already conducted 'dummy runs' to perfect the operations.

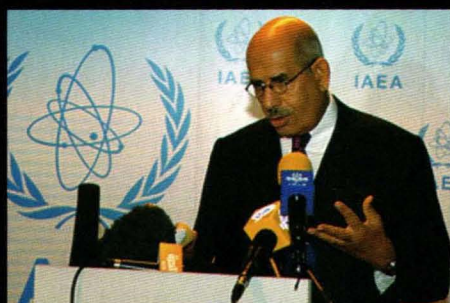
Iran's military know only too well that Israel has the capability of striking targets across the country. Some 25 years ago, Israel's air force attacked Iraq's Osirak nuclear reactor and effectively ended that country's nuclear programme. However, Iranian intelligence advisors, fearful of a similar reaction have located many nuclear facilities in remote locations, including a number that are underground and relatively safe from airborne attacks. Some in the media believe these sites would be vulnerable to ground-based operations, though this is hardly likely. Iran has considerable forces it can rely upon in the event of such an attack.

Mossad Eyes Iran's Nuclear Sites

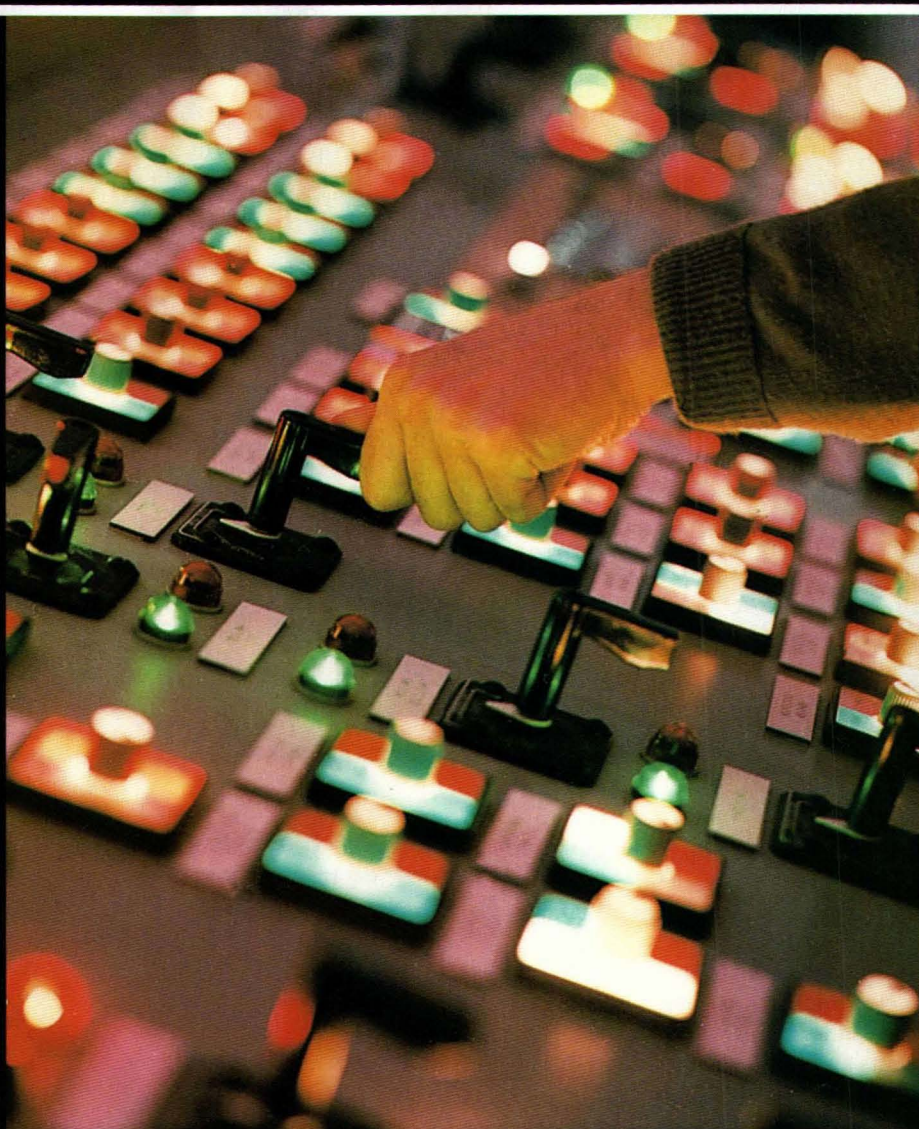
Considerable intelligence has been gleaned using a previously unknown unit attached to the Mossad. In 2005, Israeli intelligence officials concluded

OUT OF

Iran is close to acquiring a nuclear potential. It is believed that a surveillance unit attached to the Mossad was despatched to undertake a most dangerous mission - identify nuclear sites or research facilities not yet identified by the IAEA. More controversially, one unit apparently operated from northern Iraq and was central to communications and signals intelligence. The undercover units are reported to have identified several hitherto unknown uranium enrichment plants. The information has reportedly not been forwarded to the IAEA.

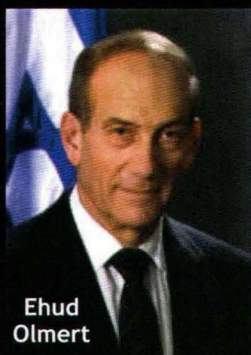


March is a critical month. Iran has already confirmed it will have all the necessary components in place to start uranium enrichment. Tehran says its nuclear programme is peaceful, but even the head of the International Atomic Energy Agency (IAEA),



TIME?

Mohamed ElBaradei, warned that the world was "losing patience" with Iran. He is set to present his next report on Iran's nuclear programme in March.



Ehud Olmert

March was also identified as a crucial period by Aharon Zeevi Farkash, director of Israeli military intelligence. He warned the Knesset: "If by the end of March the

international community is unable to refer the Iranian issue to the United Nations Security Council, then we can say the international effort has run its course." Many observers regard this remark as more than interesting, though some believe it is a ruse that will see an already jittery Iranian defence force put on alert. Intelligence watchers say Israel is 'infamous' in the trade of disinformation and the rhetoric could get Iran back to the negotiation table.

Diplomats in Israel have dismissed reports that an attack plan has been agreed. "This is ridiculous. I do not know of any decision. I think [reports]

entirely baseless," said Israeli Deputy Prime Minister Ehud Olmert. However, he was concerned about the Iranian nuclear programme. "It is true that Israel is entirely unhappy about the developments with Iran."

Most observers believe any pre-emptive strike will be carried out by the Israeli Army's 'Unit 262' - a highly trained Special Forces group that will help direct airborne operations, almost certainly conducted by the Israeli Air Force's 69 squadron. The fighter wing can reach Iran and return safely without having to refuel, though it will have





to overfly other Middle East nations to reach its targets. A situation that together with air strikes would lead to massive tension in the area.

Any attack on Iran's burgeoning nuclear industry will open Pandora's Box. Yet Israel fears that recent developments and a lack of ambition to halt Iran's nuclear programme will be disastrous for Tel Aviv. In October 2005, Iran launched Sinah-1, essentially a communications satellite that can double as a surveillance device (see Eye Spy 37).

In December 2005, Russia agreed to sell Tehran Tor-M1, an advanced system capable of destroying incoming weapons, including laser-guided bombs. An Israeli Air Force official admitted that once Tor-M1 is fully operational, any potential strike against Iran's nuclear sites would be vulnerable. "Once the Iranians get the system it will make our

IAF F-15I RA'AM [THUNDER]



Boeing's F-15E Strike Eagle entered service with the Israeli Air Force in January 1998, and was designated the F-15I Ra'am [Thunder]. The F-15E Strike Eagle is the ground attack variant of the F-15 air superiority fighter, capable of attacking targets day or night, and in all weather conditions. The F-15I serves alongside the F-15C, which has seen considerable combat since its introduction in 1976.

life much more difficult. The system can be installed quickly and we can't waste our time on this one..." Just what "this one" means is open to conjecture.

Israel's general election just happens to fall on 28 March 2006. One possible candidate opposed to Iran's nuclear programme is Benjamin Netanyahu. He said if Sharon does not take action against the nuclear sites "then when I form the new Israeli government, we will do what we did against Saddam's reactor..."

Tehran has always insisted its nuclear programme is designed to generate power. This in itself posed problems for Tel Aviv's

watchful analysts. However, combined with Tor-M1, a prolific satellite programme and a new generation of rockets that can easily reach Israel and beyond, worrying tremors are now spreading beyond Israel's intelligence industry.

British Intelligence Assessment Warns of Iranian Nuclear Missile

According to a leaked 55-page British Intelligence Assessment dated 1 July 2005, Iran has been traversing the globe in search of acquiring the necessary equipment to build and launch a nuclear bomb. Several European countries have cooperated in an attempt to identify numerous companies who may be innocently providing expert knowledge and technology to Tehran.

MI6 has played a leading role in the intelligence gathering that spans several continents. It notes that dozens of Chinese front companies have successfully negotiated contracts - all for North Korea's nuclear programme. However, it





The decision by Iran to resume nuclear research will almost certainly lead to more tension and debate at the United Nations



On 10 January 2006, Iran removed the IAEA seals at its Natanz nuclear facility (above left). These seals - to shut down equipment for making centrifuges for the enrichment of uranium - were affixed two years ago by the UN nuclear watchdog's inspectors at the subterranean Natanz facility. Iran announced it was resuming its nuclear research programme.

Britain's Foreign Secretary, Jack Straw, together with his German counterpart, Frank-Walter Steinmeier, said Iran "had crossed a line."



Bushehr nuclear facility, Iran

is the information concerning Iran that has worried so many governments.

According to the assessment, Iran has created an "extensive network" of front companies and academic firms with the sole purpose of "nuclear weapons, missile development, and biological and chemical weapons arsenals." It continues: In addition to sensitive goods, Iran continues intensively to seek the technology and know-how for military applications of all kinds."

The report provides an astonishing list of "scores" of Iranian firms and institutions that have been helping Tehran's nuclear ambitions. More disturbingly, representatives of these establishments have already made good relations with some of the West's primary universities



Iran says its nuclear research is aimed at generating electricity

researching a variety of subjects associated with nuclear and military programmes.

MI6 have also provided intelligence on Iran's wind-tunnels which are used to augment and test missiles, and various other programmes linked to missile development and rockets. One rocket known as Shahab [Shooting Star], will have the capability to reach countries such as Austria and Italy. The intelligence service also notes that North Korea continues to benefit from supplying equipment to Iran.

PROFILING A TERRORIST

LEARNING AND
UNDERSTANDING
INTELLIGENCE



In this training brief, the process recognising the characteristics of terrorists and terrorism will be explored. We will research some of the features that seem to be a common thread in known and suspected terrorists. We will look at how profiling is currently achieved and how the information is then used. We will also look into the recent changes to terrorist profiling and why these changes were necessary.

Before 9/11, the practice of racial profiling as used by police and others was considered unacceptable and even illegal. Today, adjusted profiling practices are being used to protect the country from the now all too real threat of terrorist activity. With the numerous threats that are possible in today's society, it is necessary for the government to vigilantly watch for any suspicious persons or activity. We are waging an overt war against terrorists and terrorism, but the enemy in this war is a concealed and yet obvious threat. This 21st century enemy forms hidden cells of terrorists who are preparing for and awaiting the right time to strike. Ideally, it would be best to catch such a threat before it becomes a reality. In order to accomplish this daunting task, guidelines of terrorist profiling are being developed and continually revised. In these methods of profiling, red-flag traits and activity signals are combined to single out possible threats to our society.

Terrorist profiling is no longer a matter of picking out only obvious signals of suspicion. We are no longer living in a world that can be naïve to the reality of our vulnerability. Since 9/11, the profile guidelines must be broadened to include more obscure activity and individuals or groups who try to blend into our own way of life. A terrorist profile now includes not just those in training camps overseas, but suspicious (or even not so suspicious) people using our own country's various methods and centres of learning to prepare for actions against us.

Terrorist profiling is NOT simple racial profiling where a person of a certain descent, religion, colour or creed is automatically singled out. The United States, for example, is home to a vast array of peoples with different practices and backgrounds who enjoy freedoms that do not exist in other parts of the world. Because of this, looks alone are not an acceptable single point of reference when it comes to suspecting a person or group of persons of terrorist or threatening activity. Unfortunately, media portrayal has caused many innocent persons of Middle Eastern appearance or background in general, to be categorised by society as "suspicious". We must be sure to protect rather than automatically label. This is why terrorist profiling **MUST** include expanded categories beyond race. ➤



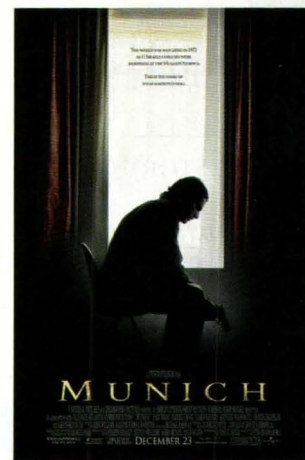
OFF THE INTELLIGENCE RECORD

MIG RECRUITING ACROSS UK

LONDON: An MI6 recruiting officer reportedly met with a reporter from the Peterborough Evening News to explain the benefits of joining the Secret Intelligence Service. The official "dropped in" to encourage the town's Asian folk to consider a career in intelligence. He noted Peterborough, situated in Cambridgeshire, had excellent transport links to London. Once famed for its covert and shadowy recruiting techniques, MI6 or SIS as it is also known, recently opened its web site in a desire to present a more public face. The organisation has received thousands of enquiries from people wanting to join the world's most famous intelligence service.

1972 MUNICH OLYMPICS ATTACK

TEL AVIV: Steven Spielberg's new movie Munich, which focuses upon how Israeli intelligence responded to the 1972 terrorist attacks at the Olympic Games in Germany, has received a mixed response - reportedly from those with inside knowledge of the affair. Eleven Israeli athletes were murdered by Palestinian terrorists. Within days, Israel vowed revenge. An elite unit was created to hunt-down those responsible, but some observers say the group killed a number of people not directly involved with the atrocity. Aaron Klein, an author whose book was published just days before the film's release said: "The fact is that the people they killed weren't involved in Munich. But at the time they thought they were and didn't care too much about it." Mr Spielberg described Munich as a "prayer for peace" and believed it would generate a constructive debate about the incident and what followed.



MIG STATION CHIEF - LIFE IN DANGER

ATHENS: Following recent disclosures by the Greek newspaper, Eleftherotypia, concerning the alleged mistreatment by MI6 and Greek intelligence of 28 Pakistani men in and around Athens, the newspaper has angered London by publishing a front-page photograph of the alleged MI6 Station Chief running in a race. The official, who has already been recalled to the UK, is now in danger, according to Whitehall sources. It is understood the photo was handed to Eleftherotypia by the lawyer, Frangiskos Rangoussis, who is representing the men. The migrant workers say they were seized just days following the July 2005 London attacks. Senior British officials have rejected the claims and condemned the newspaper's action as "grossly irresponsible." (See also page 63)

CIA SPY FLIGHTS AND 'PRISONS'

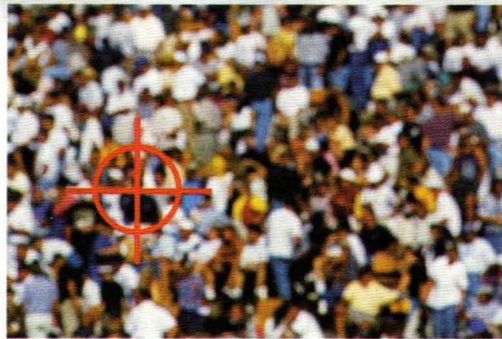
BRUSSELS: The on-going controversy about CIA flights inside Europe, especially those linked to the transfer of suspected terrorists, is to be officially investigated by the European Parliament. The move could embarrass those European countries who claim they had no knowledge of the flights.



In a related move, Europe-wide warrants have been issued for the arrest of 22 CIA officers who allegedly kidnapped Abu Omar from a Milan street in 2003. Omar was flown to Egypt for interrogation. The new warrants allow for the suspects' detention anywhere in the 25-nation EU, a prosecutor said. The Italian Government will not request Washington hand-over the officers. Intelligence sources say that the operation could not have been carried out without some prior knowledge of the Italian security services.

TERRORIST CHARACTERISTICS AND IDENTIFICATION

A profiler must have access to the most sensitive investigative materials from past terrorist attacks and activities in order to develop a sound assessment and model. This is the greatest challenge in developing a character map and profile of terrorists.



Confidential & Proprietary All Rights Reserved

HISTORY OF PROFILING

The history of profiling by law enforcement can be traced back to the 1950s.

In 1956, a rash of bombings in New York had the authorities puzzled. Investigators asked psychiatrist James Brussel, New York State's Assistant Commissioner of Mental Hygiene, to study the crime scene photos and notes from the bomber. During the investigation, some of Brussel's predictions were simply common sense while others were based on psychological ideas. In the end, however, the profile he produced proved very accurate and George Metesky - 'the Mad Bomber' - was arrested. In the following decades, police continued to consult psychologists and psychiatrists to develop profiles of particularly difficult-to-catch offenders. This was the foundation of criminal profiling.



James Brussel



George Metesky

WHAT EXACTLY IS TERRORIST PROFILING?

Terrorist profiling is the art and science of *intuitive analysis*. It is a methodical

process that is used to uncover common terrorist behaviours, based on information collected from previous interviews with captured terrorists, evidence at the scenes of attacks, and attack victims. Patterns of known behaviours and emotions suggested by historical activity, scenes, and victims are then used to create templates from which we can infer characteristics about current activities and individuals. These patterns are inferred from reasoning about initial statistical data on specific terrorist behaviour. In any event, terrorist profiling is generally the result of statistical analysis, and/or reasoning in historical data.

EXAMPLES OF TERRORIST PROFILES

While in-depth data on terrorists and their techniques is not in abundance, there is enough data to derive some critical intelligence and create a base profile. Three general categories of profiles are identified below.

Please note: Other unique traits and characteristics are known but are classified.

Terrorist Personal Profile

- Predominantly from the Middle East but groups and individuals exist throughout the world
- Predominately Male
- Between the ages of 21 and 35
- Mostly unmarried
- Most are fundamentalists
- Some university education
- Upper middle class families
- Has a revolutionary ideology
- Live an average lifestyle - blends in
- Terrorists are not initially psychopaths

- Dysfunctional family backgrounds
- Joiner - a person who seeks out participation in groups
- Difficulty forming consistent group identities outside the home
- Most terrorists are not obviously or consistently mentally ill
- Slightly less socially interactive (not loners though)
- Active lifestyle not a recluse

There is as of yet no identified universal terrorist personality pattern.

TERRORIST ATTACK PROFILE

Terrorist attacks are typically carefully planned and well-organised making effective investigation and prevention extremely difficult. Attack criteria are:

1. The attack must be strategic.
2. The attack must be symbolic
3. The attack must be catastrophic

SUICIDE BOMBING PROFILE

- The terrorist himself chooses the time and place of action, according to the prevailing circumstances.
- Simple and low cost operation - requiring no escape routes or complicated rescue operations.
- There is no danger of the terrorist being captured and giving away important information.
- Immense impact on the public and the media.

EXPLOSIVES

Triacetone-triperoxide (TATP), a relatively difficult-to-detect explosive material commonly known as acetone peroxide, is the most common explosive used by terrorists. TATP is one of a group of explosives based on the unstable peroxide group of compounds.

Profiling is an ongoing process. The method of "exploration and exploitation" has been suggested as a relatively adequate way to continue to build profiles of terrorists using the information gleaned from those individuals involved in 9/11. Exploration tracks activities of known terrorist groups and organisations. Information obtained via



exploration helps create better profiles. Exploitation also uses the information gathered from exploration to target searches more effectively. Using these two practices together forms the main target profile. However, in order to address the problem of outside operative recruits sliding through the system and to discourage people outside of the profile from being recruited, other profiles must be continually created, offered and monitored. If these methods working in tandem deter outsider recruitment, the basic target profiles will in turn be more effective.

WHERE HAS TERRORIST PROFILING BEEN USED?

The most widely known case where terrorist profiling was used occurred in the United States. The case was that of the Unabomber, probably the most famous domestic terrorist in history. By the time he was arrested in April 1996, he was responsible for a 17-year-long bombing cam-



Theodore John
Kaczynski - the
Unabomber

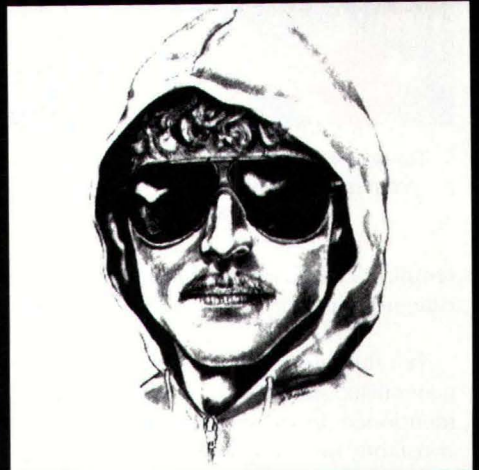
paign. In that time, he had carried out a total of 16 attacks which left three people dead and 23 injured. The Unabomber investigation cost over \$50 million, making it, at the time, the most expensive manhunt in US history.

Note: An offender profile of the bomber was first developed by the FBI as early as 1980.

The tragedy of 9/11 prompted authorities in the US and its allies to employ terrorist profiling techniques. In this case, descent and heritage does come into play when looking at former terrorist activity, and it combines with other factors to provide a generalised profile of known terrorists associated with the dramatic events of 2001.

It is a fact that the 9/11 terrorists shared certain common threads of ethnic and religious backgrounds. The terrorists fell into specific categories which included being ardent followers of Osama bin-Laden, the leader of a group called al-Qaida, and being members of the extreme Taliban, based in Afghanistan. With this knowledge, a very basic

THE UNABOMBER



THEODORE JOHN KACZYNSKI - accused of being the shadowy Unabomber who bedevilled authorities during an 18-year-long spate of bombings - acquired a Harvard degree at age 20. He could have had a dazzling academic career at one of America's top mathematics departments. But he chose another path: that of a recluse who shunned family and friends.

Some 18 months after Kaczynski's arrest at his remote, book-filled Montana cabin, the suspect has remained as silent in his prison cell as he had been during his 25-year-long, self-imposed exile.

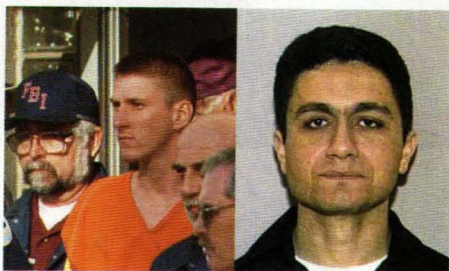
To the FBI, Kaczynski, 55, was the prize at the end of the nation's longest, most expensive hunt for a serial killer. Officials point to the mountain of evidence uncovered at the cabin - including the master copy of the Unabomber manifesto and the typewriter used to create it. In the eyes of federal investigators, Kaczynski is a cold, calculating, evil man whose contempt for technological advances led him to mastermind the bombings that killed three and injured 29.

To his family, Kaczynski is a sad, tortured man - a mathematical genius who swiftly climbed the academic ladder even as he became an emotional cripple. He had penetrated the mysteries of a complex science but never savoured the simple joys of love and friendship.

The real Ted Kaczynski may forever remain an enigma, but to the brother who made the painful decision to turn him in, one memory from nearly a decade ago stands out: In an interview with the *New York Times*, David Kaczynski recollected the time when he came emotionally close to his only brother:

It was during a visit to the Montana cabin. David was sawing wood when the work table collapsed, taking him down with it. Ted ran over, asking, "Are you OK?" David replied that he was concerned about the saw, one of his brother's few tools. "The hell with the saw. Are you OK?" David quoted his brother as saying.

"He touched my shoulders... It was incredible, and touching, and human." CNN



Timothy McVeigh Mohammad Atta - both from lands far apart - but equally as dangerous

template can be formed to begin to categorise and profile suspicious persons.

Even though we can come up with a generalised profile such as that already mentioned, terrorist profiling must be a constantly metamorphosing process that does not stick to rigid factors. The boundaries of standards used in the process must not be absolute since there is no way for the process itself to be entirely hidden from the terrorists. These groups are well aware of the types of persons being profiled, and the goal for them would be to get by undetected and carry out their mission. Terrorist groups can easily recruit people who fall outside of the profiled expectations and catch the country by surprise.

IMPLEMENTING TERRORIST PROFILING

Using terrorist profiling to uncover a specific threat before it becomes reality is

Examination



TEST YOUR SKILLS

a difficult task when you consider that all terrorists have to do is simply find someone outside of the mold to carry out their plans. However, used in combination with other protective measures, profiling can be an important part of a safety net protecting nations from a reoccurrence of the devastation brought on by attacks such as that of 9/11. For instance, suspected groups or individuals can be monitored using high tech equipment and/or numerous intelligence gathering and espionage techniques. However, as effective as these methods may be, this still leaves the problem of missing those who fall outside the target profile.

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 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 Terrorist Profiling 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) can also be downloaded at www.eyespyimag.com

For additional training briefs visit:
www.spy-ops.com



CONCLUSION

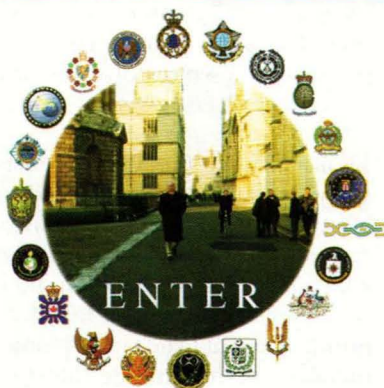
Recognising characteristics of terrorists and terrorism can seem simple to do but becomes more complicated as it is put into practice. Although profiling can create a somewhat detailed picture of a suspected terrorist based on past events, it is easy for terrorist organisations to create a loophole in this system by picking someone outside of the target profile to carry out missions. Revised profiles can be developed using methods of exploration and exploitation. These methods are put into practice by focusing on the target profile while using alternative profiles randomly to deter recruits who do not fit the basic profile criteria. By using such measures, better and more focused profiles can be created and more effectively used to weed out threats to our safety.

COURTESY: FEMA



Aftermath of 9/11 attack

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



Welcome to *Eye Spy* Magazine

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

EYE SPY SHOP

PROFESSIONAL

Professional surveillance and espionage equipment available from Eye Spy.

Check out our new range of products on: www.eyespymag.com

TRANSMITTERS & RECEIVERS

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**

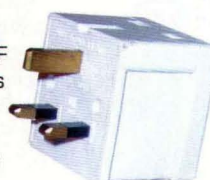
Order Code: LS-CCT UK £195.00
USA \$350.00 ROW £199.00

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

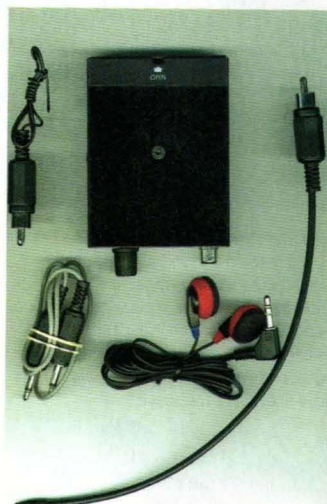


Built by specialists and used across the world

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.

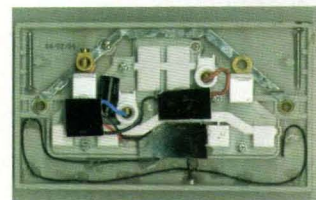
Powered by a 9v battery, the unit has a range of 400 metres - comes with jack-plug so you can record transmission and luxury earphones for privacy - all contained in a solid case.

FOR OUR FULL RANGE OF TRANSMITTERS AND RECEIVERS VISIT www.eyespymag.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 effects you.

MAINS-DOUBLE SOCKET TRANSMITTER



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



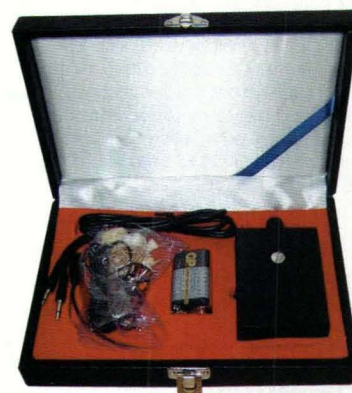
UHF CALCULATOR TRANSMITTER

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



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



EYE SPY ON- LINE

CHECK OUT OUR MASSIVE NEW
RANGE OF SURVEILLANCE
PRODUCTS AT

www.eyespyimag.com

**MINIATURE SPY VIDEO-CAMERA -
READY TO USE IN SECONDS**

EYE SPY READER OFFER



LESS THAN HALF PRICE!

This superb wireless colour video camera is the perfect low-cost solution for covert surveillance. Ready to use in seconds and easy to install. Simply position the camera facing a location you wish to observe and the receiver into a TV monitor. The camera can be concealed easily and comes with full audio capability. Ideal for home or business security.

The unit retails at £150.00 (\$300.00)
Eye Spy readers can purchase this camera and all accessories for less than half price!

Order code: LS-ESSCAM
UK £69.99 USA \$145.00 ROW: £74.99

SURVEILLANCE ACCESSORIES



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

DIALLED NUMBER DECODER Portable Touch-tone Decoder

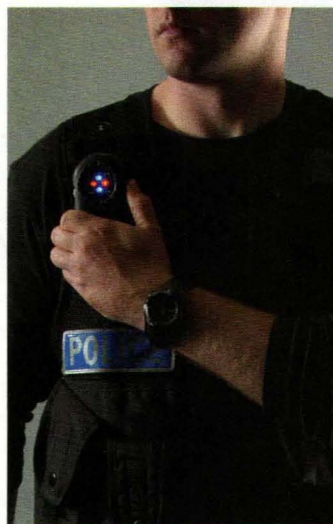


The remarkable tool devised by the security services, decodes and displays telephone numbers from tape recorded calls. This is the most accurate DTMF (tone) decoder available today. No connection is required from the actual source. Simply play your pre-recorded tape and the unit will decode and instantly display on the DIGITMASTER'S 16-digit LCD display. Works well with long-play tape recorders and noisy scanners.

Absolutely ideal for covert surveillance when you need to monitor what numbers are being called by a specific phone. Can be used with recordings made from any of our transmitters or even our parabolic mic!

Order code: TX-DND £199.00 USA \$225.00 ROW £200.00

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.eyespyimag.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

nitepalm

PARABOLIC EAR SOUND SYSTEM



The Parabolic Ear Sound System is an exceptional portable and rugged parabolic microphone which is the 'price buster' of competitive models. The detachable cone is only 12 inches in diameter and is constructed of waterproof, shock proof material. This product increases sound 37 times and, in certain cases depending upon other surrounding noise and wind, you can pick up a bird call at 400 yards. Our Parabolic Ear uses a very sensitive microphone with intricate circuitry to amplify sound (do not confuse with cheap look-a-like toys that are on the market). The sounds are transmitted to an extremely high grade amp and then to a quality headphones set which includes an automatic safety shut-off that prevents harmful loud sounds from reaching the user's ears. The dish helps pinpoint and directionalise sound and reduce noise background. Unit has tape recorder patch cord for tape recording.

Features: Super sound amplification; focus on sounds in the direction you point the microphone; automatic circuit shuts out sounds over 95 decibels so loud sounds are not amplified; independent volume control allows you to select best amplification for each ear so you can adjust for individual hearing differences; output Jack allows you to record what you hear; wrist straps accessory attach the microphone to your forearm for hands-free operation.

Operates on one 9 volt battery for 40 hours of continuous use.

Order Code: TX-PESS
UK £175.00
USA \$196 ROW £185.00

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

CELL PHONE VOICE CHANGER

Available for the first time - a quality telephone voice changer designed specifically for mobile and cordless phones. The voice changer has a 'normal' setting plus four different voices. Now you can answer your cell phone or call someone on your cell phone without anyone



recognising your voice. Just switch a button and completely change your voice. Universal to fit all mobile/cordless and cellular phones. When you are not using the item as a voice changer, it also makes a great hands-free head set for your cell phone. Just switch the unit to normal voice and speak hands-free.

Easy Installation: Most mobile phones have a mating DC power plug for hands free headsets. This is the same power plug used by the voice changer. For cordless phones just plug the DC jack into the mating DC Power (120) plug on cordless phone handset.

Order code: TX-CPC UK \$75.00 USA \$84.00 ROW \$80.00

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 \$72.00

Spy Phone - TelSpy Motion Activated Intrusion Notification System

This standard 'trim line' type telephone features a built-in PIR motion sensor. If an intruder is detected within a 30 foot range, TelSpy calls a preset telephone number and allows you to listen in to the premises. Great for protection of homes, businesses, vacation homes and warehouses.

Order code: TX-TELSPY USA \$215.00



UK inquiries please email eyespy@eyespyimag.com or call 01756 770199

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

High Quality Watch Microphone

A fully functional wristwatch that houses an integrated seed microphone. The lead is concealed in shirt or jacket and can be connected to any cassette recorder



Please specify
Ladies or
Gentleman

Order Code: LS-WW UK \$50.00
USA \$90.00 ROW \$55.00

COMPLETE WITH RECORDER
Order Code: LS-WWR UK \$90.00
USA \$180.00 ROW \$100.00

Please write for our free 32-page catalogue of specialist surveillance equipment, or visit www.eyespyimag.com to view our huge range

EYE SPY'S ENIGMA BUG World Famous Listening Device

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.

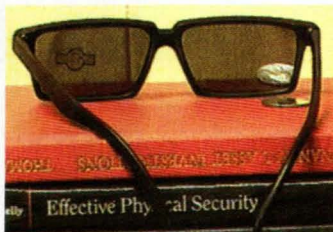


environment, allowing colleagues thousands of miles away to listen in. Similarly, simply leave the phone at a location and dial up whenever you need to listen. A superb bug used by professionals only.

Now available for the USA cell phone network

Order Code: LS-ENIGMA
UK \$295.00 USA \$599
ROW \$310.00

REAR VISION SURVEILLANCE SUNGLASSES



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

TINY TECH 16, 18 or 36 hour Quality Voice and Telephone Recorder

Smaller than a lighter, this amazing recorder holds up to 396 messages in four separate file folders. It also doubles as a covert telephoner recorder. Built-in microphone or supplied external mic for crystal clear digital recordings. Adjust the quality of recording as needed (higher quality uses more memory). All recordings can be easily uploaded to your computer for emailing or editing with the provided user friendly software. For telephone recording, the unit simply plugs directly into the phone jack. Both sides of the conversation are recorded (no beeps or tones to indicate recording) from any line in the house including cordless. Voice activation mode available. The Tiny Tech can also be used as a 64mb storage drive and Mp3 player.

Order codes:

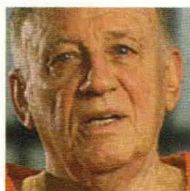
TX-TECH-16 Hours UK \$175.00 USA \$225.00 ROW \$175.00
TX-TECH-18 Hours UK \$200.00 USA \$269.00 ROW \$200.00
TX-TECH-36 Hours UK \$235.00 USA \$299.00 ROW \$235.00



UNDER COVER

BOOK RELEASES

THE IMPERFECT SPY:
The Inside Story of a
Convicted Spy
Andy J. Byers
ISBN 0-918339-66-9
Vandemere Press
Hardback 256pp

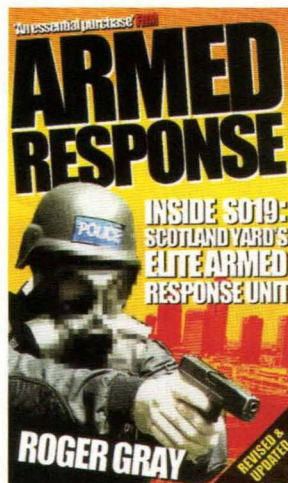


and from the author's personal observation over a five year period, combine to create a remarkably intimate look of a very public event.

The Imperfect Spy is the inside story of George Trofimoff, an American civil servant and army reserve colonel, convicted in 2001 of spying for the Soviet Union throughout the Cold War. It is a story of betrayal, greed, and treachery at an almost incomprehensible level. The Imperfect Spy is a remarkably complete look at the life of a spy, told from both Trofimoff's point-of-view and from the trial record. The author's unique access to Trofimoff's wife's comments, Trofimoff's writings,

Available from Eye Spy
Ref: ES/1133 £25.00 \$30.00

ARMED RESPONSE:
Inside SO19 - Scotland Yard's Elite
Armed Response Unit
Roger Gray
Virgin Books
ISBN: 075351110X
Paperback 352pp



Armed response tells the gripping and often alarming story of SO19, the armed response unit of the Metropolitan Police, and the Trojans, the armed response vehicles permanently on patrol. Driven by the need for experienced firearms officers to be on the scene in minutes, the Trojans are ready at all times to meet the threat of an armed incident in the capital. Following the devastating terrorist attacks on London in July 2005, the ability of the police to deal swiftly and effectively with the threat of terrorism has never been greater. The tragic shooting of an innocent man thought to be involved in the attacks only a few weeks later highlighted the unimaginably difficult task these

police officers face and the immense responsibility of protecting us from the threat of terrorism and armed incidents. This fully revised and updated edition, including a new chapter on the London terrorist attacks and their



SO19 officers

aftermath, provides a vivid and extraordinary account of the work these brave men and women undertake.

Available from Eye Spy
Ref: ES/1137 £9.99 \$20.00

THE ImPERFECT SPY



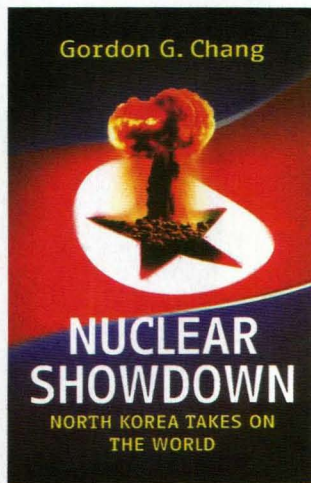
THE INSIDE STORY OF
A CONVICTED SPY

ANDY J. BYERS

NUCLEAR SHOWDOWN:
North Korea Takes on the World
Gordon G Chang
Random House
ISBN: 0091799708326
Softback 326pp

Asia expert Gordon Chang follows up his controversial success, 'The Coming Collapse of China', with the first book to discuss the full extent of the North Korean nuclear

threat, its origins, international implications, and solutions. The United States is the mightiest nation in history, yet for six decades one of the world's weakest states has challenged the superpower and kept it at bay. Today, that country also threatens to change the course of human events with an act of unimaginable devastation. Nuclear Showdown analyses the failed society

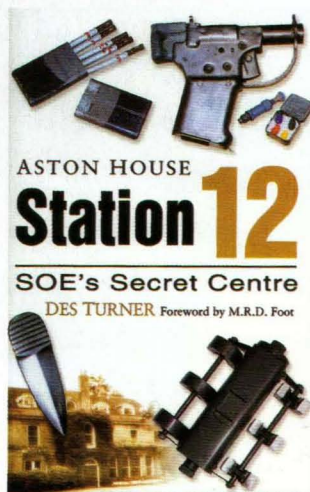


that has become the gravest threat to America and international order: North Korea. Chang's insightful book reveals the full horror of the crisis threatening to turn Asia into the world's next battleground where millions could die in hours. How can Washington stop North Korea from taking down the American-led international system? No one seems to have an answer. For more than half a century, policymakers have failed when it comes to subjugating Kim Il Sung and his son, Kim Jong Il. "Nuclear Showdown" proposes a solution that can defuse the standoff once and for all.

Available from Eye Spy
Ref: ES/1135 £17.99 \$40.00

STATION 12:
Aston House: SOE's Secret Centre
Des Turner
Sutton Publishing
ISBN: 0 7509 4277 0
Hardback 246pp

The full story of Aston House in the Second World War has never been told before. Its activities were top secret and as important to the war effort as Bletchley Park, but in a different way. Situated near Stevenage, Aston House was one of many British country houses



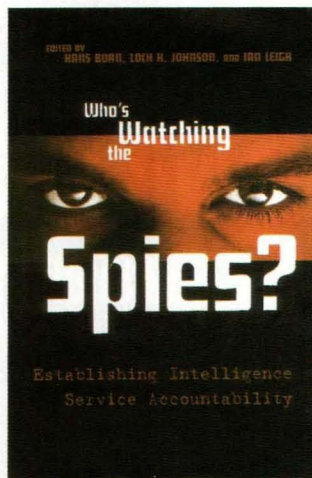
requisitioned during the Second World War by the Special Operations Executive (SOE). Known as Station 12, its task was to design and supply special weapons and explosive devices for sabotage operations against the enemy. The scientific and military personnel at Station 12 invented, made and supplied 'toys' such as plastic explosives, limpet mines, pressure switches, tree spigots, incendiary bombs, incendiary liquids and arrows, and a variety of time fuzes for the Resistance, Commandos, Special Boat Service and SAS. In the grounds of Aston House were magazines for the explosives and sheds in which to handle them, large storehouses for incendiaries and all the rest of the 'toys', and workshops for experimentation and manufacture. Station 12 designed and made up special explosive charges tailored for specific tasks or operations, including such famous special operations as the Bruneval and St-Nazaire raids, the assassination of SS Obergruppenführer Reinhard Heydrich (above), and the attack on the Telemark heavy water plant in Norway.

Available from Eye Spy
Ref: ES/1134 £22.99 \$45.00

WHO'S WATCHING THE SPIES:
Establishing Intelligence Service
Accountability
H Born, Loch K Johnson, I Leigh
Potomac Books
157488 896 x
Softback 272pp

Given recent experiences with terrorism, clearly even the most democratic societies have a legitimate need for secrecy. This secrecy has often been abused, however, and strong oversight systems are necessary to protect individual liberties. The assembled authors, each well known in the international community of national security scholars, bring together in one volume the rich experience of three decades of experimentation in intelligence accountability. Using a structured approach, they examine the strengths and weaknesses of the intelligence systems of Argentina, Canada, Germany, Norway, Poland, South Africa, South Korea, the United Kingdom, and the United States. While these democracies have experimented with methods to make intelligence more accountable, they all have different political systems, political cultures, legal systems, and democratic traditions, thereby presenting an exceptional

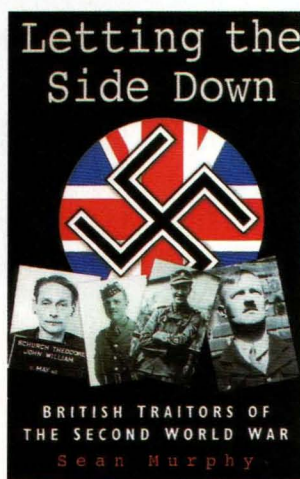
opportunity to examine how intelligence accountability evolves under disparate circumstances. The contributors draw together the best practices into a framework for successful approaches to intelligence accountability, including a prescription for a model law.



Available from Eye Spy
Ref: ES/1136 £29.99 \$60.00

LETTING THE SIDE DOWN: British
Traitors of the Second World War
Sean Murphy
Sutton Publishing
ISBN: 0750941766
Paperback

Now available in paperback, this is the fascinating story of a collection of misfits and renegades who came from all walks of life and different social backgrounds, but who all had one thing in common. During the Second World War they chose to reject their country and follow the path of treason through collaboration with the Axis powers. Altogether, about two hundred British citizens were under investigation for assisting the Axis powers. Using the case studies of the individuals concerned, Sean Murphy uncovers the reasons for their treacherous activities,

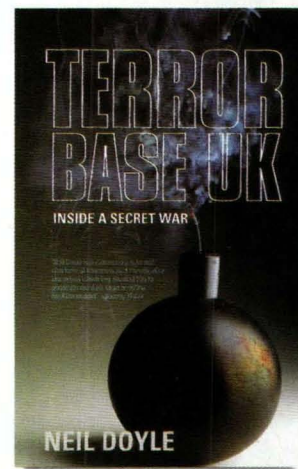


describes how they collaborated with the enemy, and come the end of the war he explores their respective fates. The stories of some of the more notorious traitors like William Joyce (Lord Haw-Haw) and P.G. Wodehouse are already well-known but also included are some of the lesser known but equally treacherous individuals.

Available from Eye Spy
Ref: ES/1139 £10.49 \$22.00

TERROR BASE UK:
Inside a Secret War
Neil Doyle
Mainstream Publishing
ISBN: 1-84018-994-0
Softback 240

Terror Base UK is cyber-journalist Neil Doyle's chronicle of the epic struggle between al-Qaida and the West. By tracking websites used by al-Qaida and other terrorist



organisations to plan, coordinate and celebrate their attacks, as well as to recruit and train their members, he is now able to reveal: how the London suicide bombings on 7 July 2005 could have been prevented; how a secret jihad army has established itself in Britain, making the country al-Qaida's European HQ details of several previously undisclosed bomb plots, including one involving chemical weapons the first documented terrorist cyber-attack; and the fatwa issued by an al-Qaida spiritual leader that pre-approves the deaths of millions of people in the West.

Terror Base UK is an action-packed tour of the secret terror war written by one of the world's leading investigative journalists. This is not for the faint hearted or for those who still believe the threat is imaginary.

Available from Eye Spy
Ref: ES/1138 £12.99 \$30.00

EYE SPY



PRODUCT REVIEW

ZAP CHECKER ADVANCED

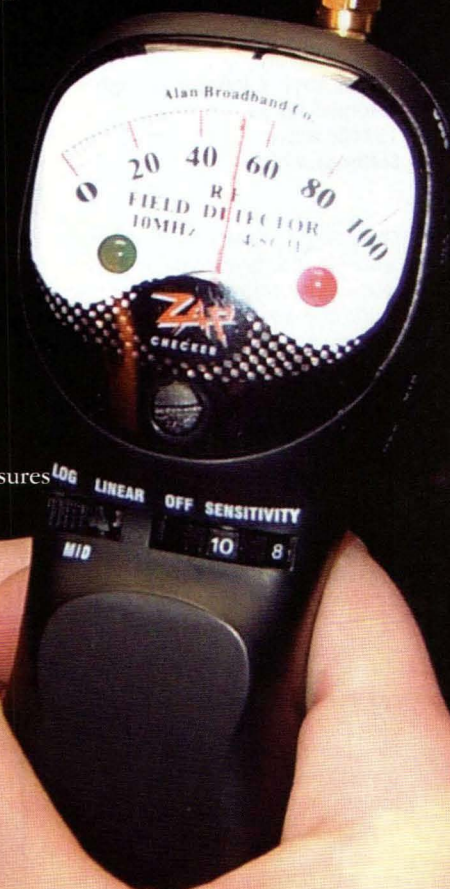
Bug and covert camera detection made easy

It's difficult to know where to start with this extraordinary electronic counter-measures device, but let's say it would certainly be high on my 'wish list'. We have all seen the hi-tech movies whereby intelligence officers 'home-in' on concealed bugs and cameras using instruments more befitting to a Hollywood B Movie: lights flicker and an audible warning sounds as one nears the bug. Tension increases and the alarm and instrumentation goes haywire. Well, Zap Checker Advanced does both of these, but it also vibrates as well and has several other 'canny' features. Utilizing new integrated circuits developed for use in cell phones and wireless devices, the unit is hundreds of times more sensitive than standard field strength meters, and more sensitive than most spectrum analysers. However, it is particularly suitable for the detection of radio frequency (RF) signals from transmitting bugs and covert cameras.

The firm that makes the Zap Checker range (Eye Spy's Shop carries several variants) makes a few boasts. The packaging says: "Zap Checker Advanced measures radiation from cell phones, microwave ovens, 'bugs' (transmitters), two-way radios etc. The range is impressive - 10MHz - 4.5GHz." It also comes with a meter and two colour LED display.

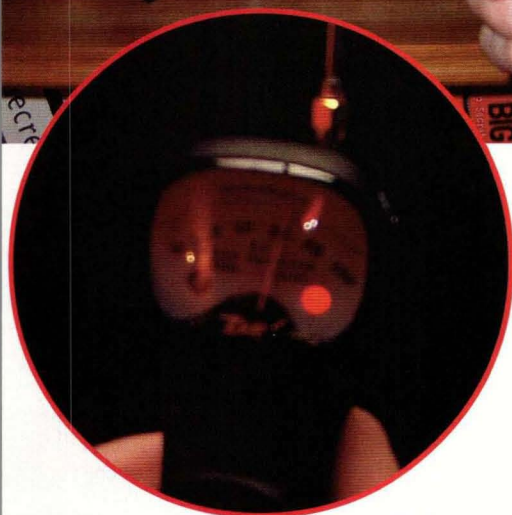
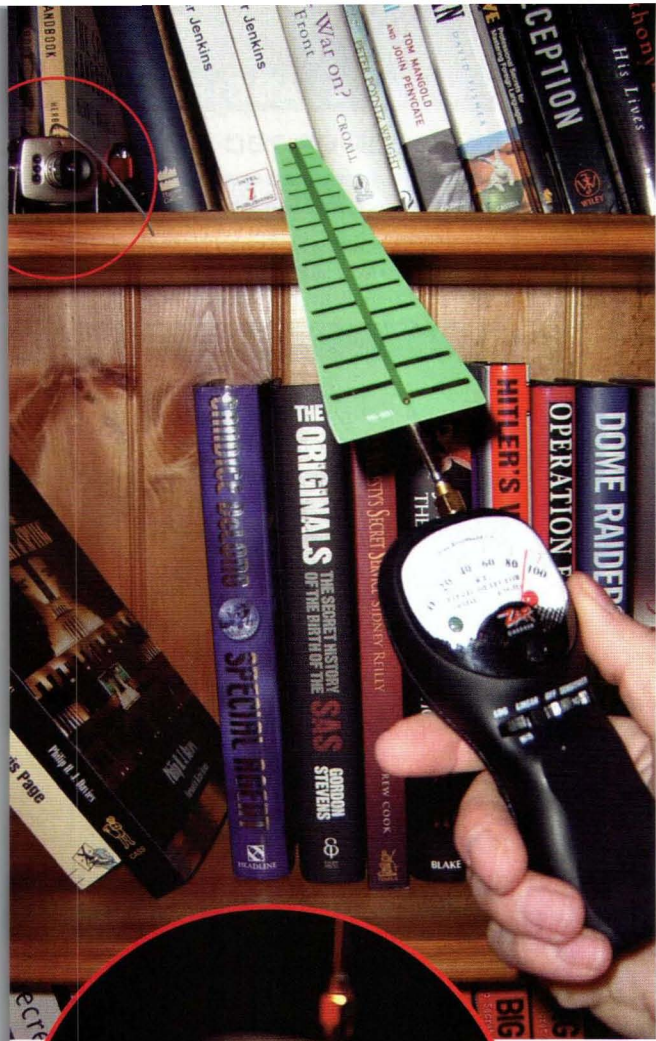
When we requested a product review, we expected quite a substantial piece of kit, especially as you would not expect much change from £450.00. When Zap Checker arrived we were not disappointed, but a little suspicious. A hand-held product with a 'Christmas-tree' like aerial did not inspire our engineer, but we were astonished by the effectiveness of this impressive 'bug hunter'.

The Zap Checker Advanced is a new generation countermeasures RF sweeper that detects and displays RF signal levels with uniquely high sensitivity, similar to a broadband receiver. It provides linear and logarithmic measurements of RF signals over a broad span of frequencies. The device allows the user to detect and measure signal strength and to distinguish between analogue and digital transmissions.



EYE SPY RATING





An Eye Spy employee was charged with hiding five espionage devices in a cluttered room some 60 feet long and 30 feet wide. Three transmitters (bugs) UHF, VHF and FM were carefully concealed behind books, a refrigerator and inside a hollowed-out stone slab. A spy camera attached to a 9 volt battery was transmitting, and just for good measure, we turned on an Enigma spy phone placed on a bookshelf.

We invited a total novice to attach the aerial to the Zap Checker and explained he could home-in on the bugs using the meter, light display or vibration facility, which incidentally can either sound a warning or operate silently, which is terrific if you need to monitor a location or check for a covert body-worn bug.

It took just seconds for the operator to locate the hidden camera. Within five minutes every bug had been discovered. Our member of staff had carried out a

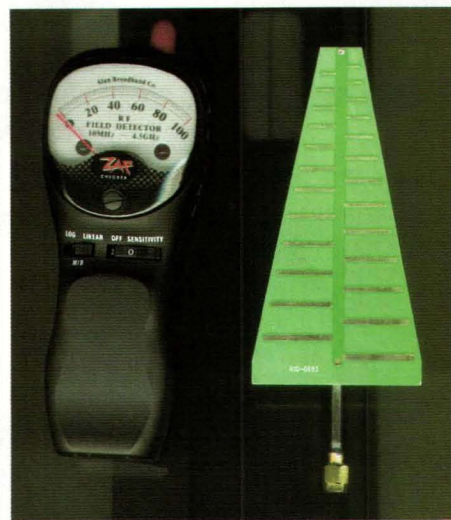
relatively tough assignment and passed with flying colours. Having the ability to reveal the presence of a bug in your office or home is one thing, having the equipment to actually find the device is far more comforting, and could provide clues as to the handler or company who actually concealed the device in the first place.

The Zap Checker Advanced is a compact battery-operated unit that can identify the simultaneous output of ALL RF transmitted signals within its wide bandwidth including cellular phones, wireless phones, analogue, pulsed, hopping, spread spectrum, trunking, TV and short wave broadcasts, computer wireless devices, wireless security systems, microwave ovens, ham radio, police and service bands, and transmitting surveillance and spying devices such as hidden cameras, transmitting bugs and covert video or data transmissions.

The Zap Checker features electronically-switched antenna selection options between its two internal antennas and its external log periodic antenna. It provides three switchable detection modes - linear (for detection from a distance), log (to sort through multiple signal sources), and mid (to home-in and pinpoint devices). It's ergonomically engineered design is small enough to fit in your pocket and it is also free-standing for convenient continuous monitoring.

Its in-built analogue meter gives a reading of radio frequency signal strength. It also provides a clearer visual display of rapid signal changes than other types of displays. Furthermore, the device has the added advantage of detecting superior weaker signals.

Continuous radio frequency signals are detected in the analogue mode. The digital mode is used when the transmitting device is broadcasting digital or rapidly pulsed analogue signals. Digital signals are distinguished from analogue signals when measurements in the digital mode are noted to be stronger than in the analogue mode.

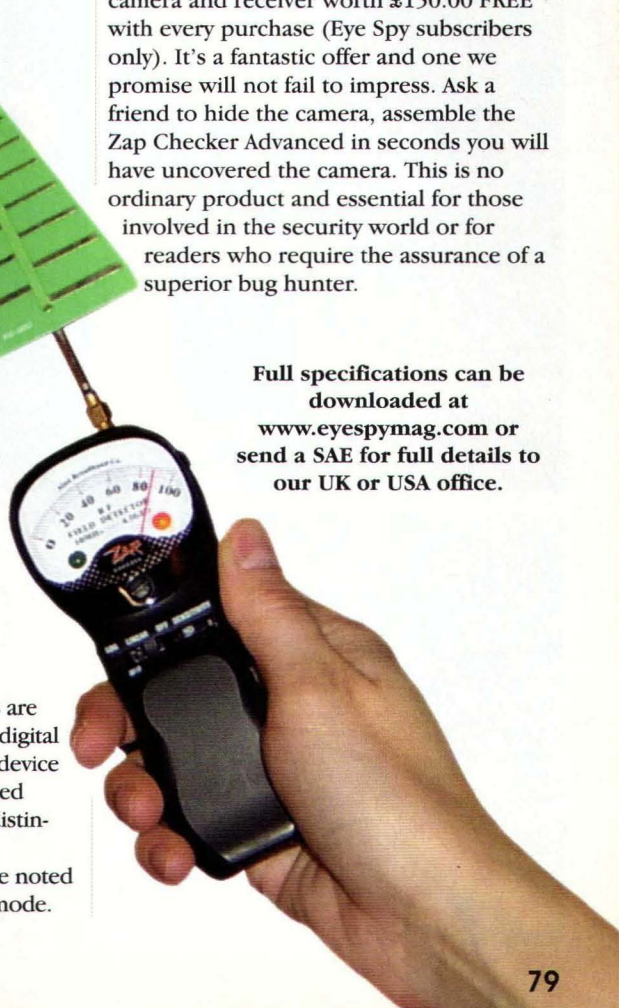


All very interesting but the outcome is the same. Zap Checker Advanced is the best physical bug hunter at its price and can easily compete with counter-measures products costing four or five times as much. The instrument is easily carried and concealed and has a plethora of supporting functions that enables the operator to determine what type of bug is in use and the frequency it is transmitting.

Operates on two AA batteries for over 60 hours. Full instructions are easy to follow and will allow the operator to use it within seconds. It's that easy.

Eye Spy is so impressed with the Zap Checker Advanced, we will supply our best-selling colour and audio security/spy camera and receiver worth £150.00 FREE with every purchase (Eye Spy subscribers only). It's a fantastic offer and one we promise will not fail to impress. Ask a friend to hide the camera, assemble the Zap Checker Advanced in seconds you will have uncovered the camera. This is no ordinary product and essential for those involved in the security world or for readers who require the assurance of a superior bug hunter.

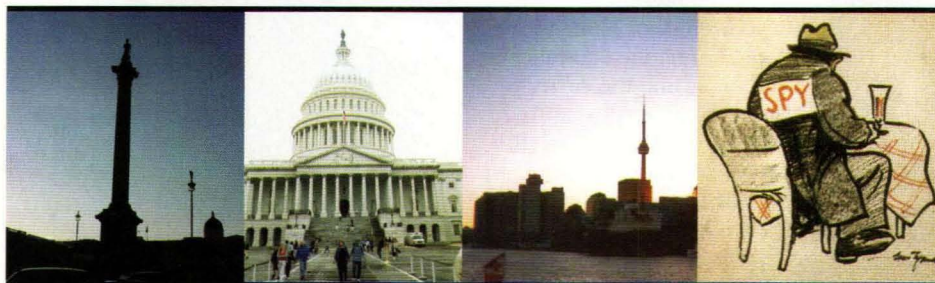
Full specifications can be downloaded at www.eyespy.com or send a SAE for full details to our UK or USA office.



• EYE SPY CLASSIFIED •

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@eyespyimag.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.

SMALL CLASSIFIEDS

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, AUSTRALASIA REST OF WORD

Eye Spy Magazine, (Classified),
P. O. Box 10, Skipton,
North Yorkshire, BD23 5US, England

SMALL CLASSIFIEDS

Eye Spy Magazine: We have a large number of readers urgently seeking issues 1, 6 and 7. If you can assist, please telephone: 01756 770199

Professional Services

KALETON INTERNET

International supplier of Internet services to businesses and individuals with special needs for security, privacy and anonymity.

- Web hosting, domain registrations and web design.
- Secure email accounts.
- Security and virus research.
- Penetration testing and ethical hacking.

Visit us now for all your online needs

Your secrets are our secrets
WWW.KALETON.COM

INTERNATIONAL SECURITY ACADEMY

VIP PROTECTION
Protection Management

COUNTER TERRORISM TRAINING
Preparatory training in Israel for Protection personnel operating in high risk areas as: Iraq, Afghanistan, Kosovo & Africa

LAW ENFORCEMENT

INTERNATIONAL SECURITY ACADEMY - ISRAEL
P.O. BOX 5833 Herzliya 46000 ISRAEL Tel: +972-9-9500969 Fax: +972-9-9573392

INTERNATIONAL SECURITY ACADEMY - EUROPE
Europe@SecurityAcademy.com
Switzerland +41 44 2110210 U.K. +44 20 75588523 U.S.A +1 202 4703189

www.SecurityAcademy.com

Deleted Text Messages Recovered

SIM CARD DATA RECOVERY

Have you ever deleted those important messages from your mobile phone and can't recover them? Did you know the SIM card has a memory chip that stores up to 20 SMS text messages as well as your mobile phone address book.



We can read the SIM card using the latest technology and software.

All we require is the SIM card which is returned in the same condition with a printed copy of the deleted messages.

For further details call 07977 477946 or visit

www.topnights.net

ijet TRAVEL RISK MANAGEMENT

Keeping you safe, healthy and productive.

www.ijet.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

ISS TRAINING LTD

The World's Premier
Surveillance Training Courses

Peter Jenkins - author of:
ADVANCED SURVEILLANCE



Tel. UK 01423 712265

THE SPYCRAFT MANUAL

THE INSIDER'S GUIDE TO
ESPIONAGE TECHNIQUES

AVAILABLE FROM EYE SPY
Ref: ES/984 £17.99 \$45.00

FOREWORD BY
RICHARD TOMLINSON
BARRY DAVIES, B.E.M.
SPY SCHOOL INSTRUCTOR

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

EYE SPY BINDERS



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

Ref: ES/099

UK £7.50
USA \$17.00
ROW £9.50



BRIXMIS ASSOCIATION



www.brixmis.co.uk



CAMP X

Visit the Camp-X
Museum on the shores
of Lake Ontario
www.camp-x.com

www.bletchleypark.com



IMAGE: LEPL/BELINDA WARREN



SPY MUSEUM FINLAND

www.vakoilumuseo.fi



[http://groups.yahoo.com/
group/enigma2000](http://groups.yahoo.com/group/enigma2000)



www.coldwar.org



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

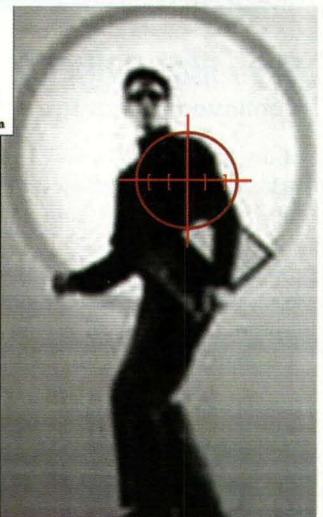
email info@tcominternational.co.uk



Enhancing
Your
Performance

Continuing Education
Available Today

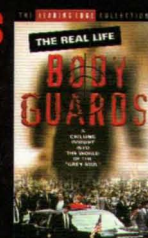
Visit
www.Spy-Ops.com to receive
your free Training Brief on
Corporate Espionage and
learn about our exciting New
Offerings.



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.

PAL VHS Ref: ES/20
UK £8.49 EUR \$9.99
ROW £10.99 USA \$20.00
60 minute documentary



These are
the real
'grey
men'
- Eye Spy

US readers note - this is not NTSC. Available
from Eye Spy - use form on page 82

technolytics

Technology
for

Intelligence

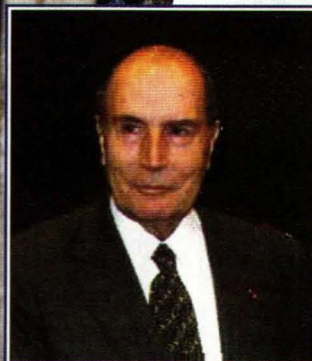
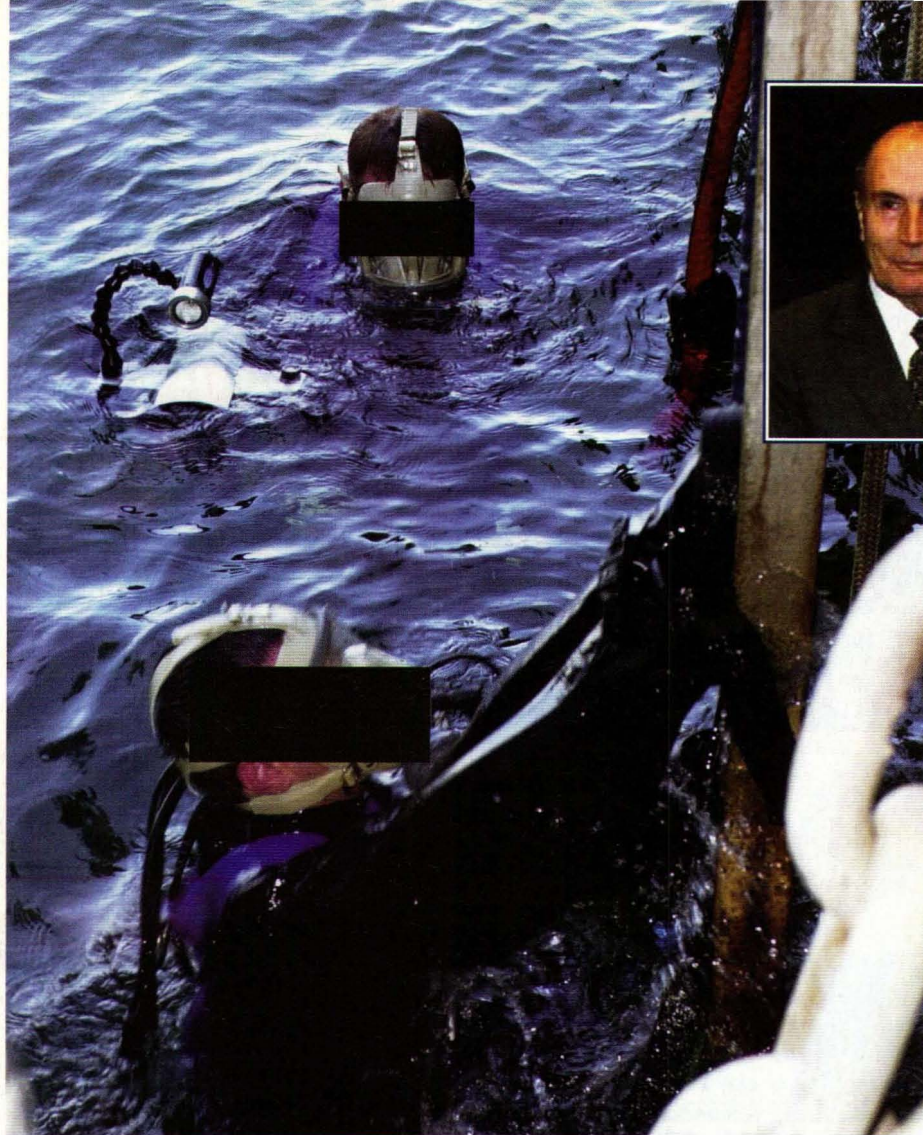
A new technology revolution is coming!

Will you lead...

follow...

or be pushed aside?

www.technolytics.com



In 2005 it emerged Mitterrand did authorise the bombing

states: "Despite all these protestations of innocence, the cumulative evidence from many quarters of French official briefing now seems irrefutable." The writer recommended "firmer action to end this debilitating campaign of smear."

By October, British intelligence had concluded the DGSE was to blame for the French reports (and the attack on the Rainbow Warrior), but the Foreign Office warned: "Allegations of British skulduggery continue to find a receptive audience in France, but have surfaced less and less frequently as French responsibility has become unmistakably clear."

In the end Mitterrand, who denied any knowledge of the Rainbow Warrior attack or the MI6 'blame game plan' sacked his defence minister, Charles Hernu, and the head of the DGSE, Admiral Pierre Lacoste.

However, in 2005 it emerged Mitterrand did authorise the bombing. Lacoste wrote in a leaked memo that the French premier demanded Greenpeace stop disrupting French nuclear weapons tests in the Pacific.

On 12 December 1987, the crippled Rainbow Warrior was sunk at Matauri Bay, New Zealand. On 10 July 1987, the new Rainbow Warrior was launched in Hamburg, Germany. France was ordered to pay Greenpeace \$8 million compensation.

MI6 - DGSE RAINBOW WARRIOR

Continued from page 41

of the Rainbow Warrior." In response, British officials explained the French reports were "pure fantasy."

Foreign Office minister Malcolm Rifkind was told by Downing Street to order UK diplomats in Paris to stop France's "campaign of misinformation." The

reports of MI6 involvement continued and Whitehall suspected officials at the French Embassy in London were at the heart of the operation. Stories that MI6 operatives were behind the Rainbow Warrior's destruction were spreading to countries all over the world. Meanwhile, French officials "denied everything."

A former classified Foreign Office document dated 4 September 1985,

OFFICIAL EYE SPY ORDER FORM

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@eyespymag.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@eyespyrsmag.com

Web Site: www.eyespyrsmag.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 Hockeimer
legal editor



MARK IAN BIRDSALL
editor



Lynn Hodgson
Canadian editor



Glenmore Trehear Harvey
associate editor



Jim Shortt
military consultant



Peter Jenkins
surveillance editor



Spiros Kaplitos
Greece editor



Donald Napier
intel news



Kevin Coleman
consultant

Director of International Corporate

Affairs: Deborah McDonald

Copy Editor: Virginia Hockeimer

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 39 ON SALE MARCH 2006

- NEW CLOSE PROTECTION SERIES
- HOSTILE ENVIRONMENT TRAINING II
- 100 SURVEILLANCE TIPS!
- HOW TO USE TOOLS OF THE TRADE
- EXCLUSIVE INTEL INTERVIEW
- WHAT NEXT FOR IRAN?
- AMERICA'S NEW DEADLY SPECIAL FORCE
- HOW TO HANDLE SUSPICIOUS PACKAGES
- ANATOMY OF INTELLIGENCE



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

EYE SPY

www.eyespyimag.com

