

The Covert World of Espionage

TM

EYE SPY

COUNTER TERRORISM



- PROFILING
- RECRUITERS
- SUICIDE BOMBERS
- SURVIVING CAPTIVITY



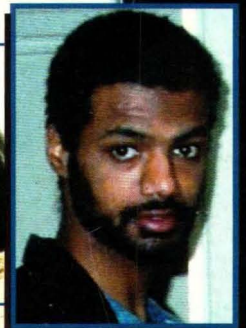
SPY features on
CIA • MI5 • FSB



MI5 MI6
1909-2009

100 YEARS OF SECRET SERVICE

Guantánamo Conundrum



NSA CODEBREAKING FINDS

- MOSSAD TARGET NUCLEAR SCIENTISTS
- HACKING THE PENTAGON
- WANTED - CYBER WARRIORS
- THE CIA DOUBLE AGENT

NUMBER 61 2009
USA \$6.50 • CANADA \$7.99



Printed and Published in Great Britain

SPY GAMES

KEEPING IT IN THE FAMILY

A jailed CIA double agent used his son to make contact with his former FSB handler to "collect his spy pension"

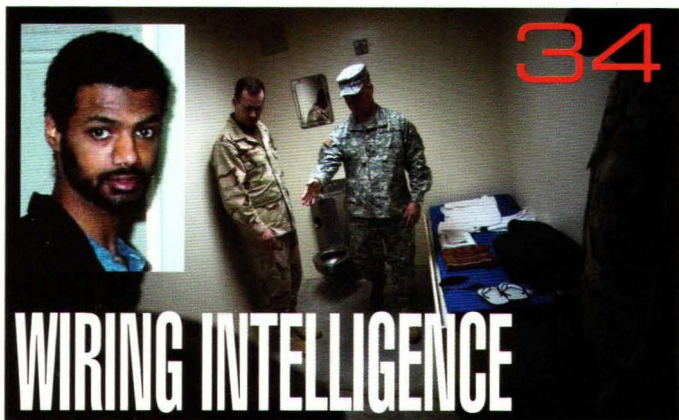


14



MUMBAI 10

Intelligence agencies fear similar city-centre terrorist attacks could happen in the West



34

WIRING INTELLIGENCE

Controversial intelligence documents, Guantanamo Bay, torture accusations and the puzzling case of Binyam Mohamed

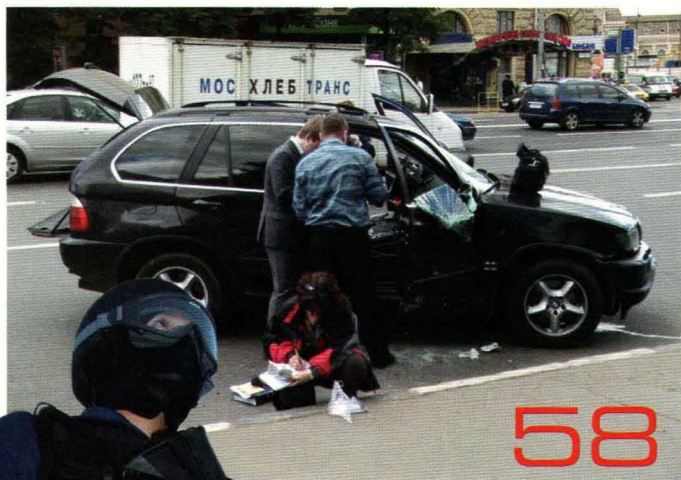


Britain's two premier spy agencies celebrate their 100th birthday

1909-2009



48



58

British military trainer Simon Atkinson, continues his fascinating series... this time he focuses on surviving captivity

HOSTAGE SURVIVAL

PART 3

AMERICAN RECRUITERS

Al-Qaida focus attention on US citizens in drive to create mainland terror cells. CIA warns of 'stepping stone' Europe



18



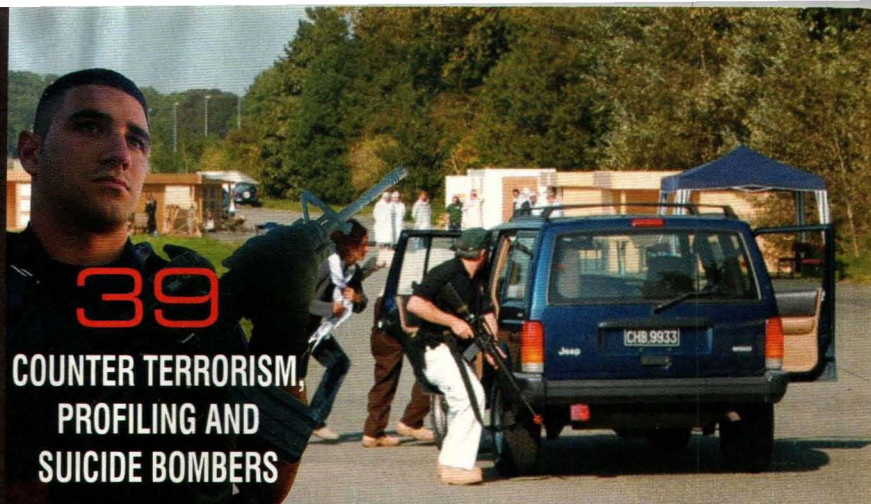
'Gems' in the NSA close

New Letter from Fort Mead

David Hamer looks at some recent discoveries made at the NSA's museum, and discusses a few Pearl Harbor conspiracies!

70

EYE SPY



39 COUNTER TERRORISM, PROFILING AND SUICIDE BOMBERS

4 FINANCIAL MELTDOWN AND TERRORISM
Dennis Blair, the new US director at the Office of National Intelligence, has warned the economic slowdown will probably lead to more terrorism and criminality

6 MOSSAD CHANCE TACT OVER IRAN?
Intelligence sources in Tel Aviv say the Mossad has initiated a new operation intended to slow down Iran's "race for the bomb"... by targeting scientists

8 EX-KGB SPY BUYS INTO BRITISH MEDIA
Former London-based KGB officer Alexander Lebedev, has purchased the capital's most famous newspaper - the London Evening Standard for just £1

17 DOUBLE AGENT
Former CIA Station Chief Harold James Nicholson was arrested at Dulles Airport in 1996. The career officer was attempting to board a flight to Switzerland. From inside jail, he used his son to collect his "FSB pension"

20 CLEAR AND PRESENT DANGER
Former Director of CIA (D/CIA) Michael Hayden's 2008 message about the new operatives of al-Qaida

21 THE HACKER MAN
Glasgow-born Gary McKinnon faces extradition to the USA after hacking into Pentagon computer systems and causing massive disruption. He says he was looking for evidence of flying saucers

26 TAKING PICTURES AND SECTION 76
A new law - Section 76 of the Counter Terrorism Act - has been met with anger by photographers and journalists alike. The law, brought in essentially to protect officers participating in operations, could be abused... at least according to civil liberty groups and media unions

30 CAMP 30 - BOWMANVILLE
An iconic Canadian building and area once used to hold WWII German PoWs, is to be demolished by a developer. Eye Spy reports why readers should protest...

46 URBAN WARFARE
Terrorists launch another audacious city centre attack - this time against an international cricket team playing in the Pakistan city of Lahore. Security chiefs believe such an event could now happen in the West

56 EYE SPY PRODUCT REVIEW
Peter Jenkins tests a new self-contained covert camera that is both affordable and produces excellent results - plus there is a reader offer on the PI Camcorder Stick

58 US EMBASSY FINDS NEW HOME NEAR MI6
After an association of some 200 years in Mayfair, London, terrorist concerns have led the US Embassy to seek out a new home... favourite is a site near MI6's headquarters

75 WANTED - CYBER WARRIORS
Intelligence analyst Kevin Coleman looks at the intel world's response to the emerging Cyber Cold War. It's also a good time to find employment in one industry that is burgeoning... countering computer hacking



HEADLINERS



•4 Dennis Blair •5 Leon Panetta •9 Yuri Fedotoc
•15 Nathaniel Nicholson •21 Gary McKinnon

•48 Sir Mansfield Cumming •48 Sir Vernon Kell •70 Patrick Weadon

regular features

4 Intelligence Briefings; 6 Intelligence Extra; 28 Eye Spy Back Issues; 66 Eye Spy Shop;
68 Subscribe; 79 Eye Spy Classified

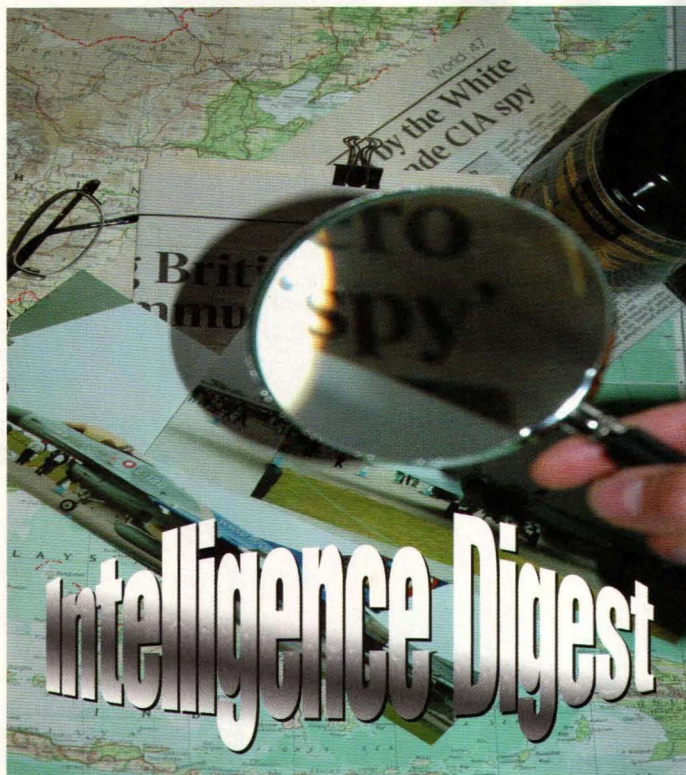
EYE SPY EDITORIAL ACCUSATIONS OF MI5 TORTURE



The case of former Guantanamo Bay prisoner Binyard Mohamed is both controversial and potentially disturbing. But it is far from simple. Mohamed was linked to the Chicago residential tower block terror plot by US intelligence - through association with a young Chicago thug called Jose Padilla. All charges against Mohamed, who was arrested travelling on a false passport by Pakistan security services, have since been dropped. While the Ethiopian-born Mohamed is back in the UK, Padilla, who the FBI originally said was going to detonate a "dirty bomb" in the building, was jailed anyway... but for lesser charges.

Mohamed and his supporters have accused MI5, or at least one of its "agents", of "complicity in torture". I'm sorry, but MI5 as an organisation does not torture anyone. It will, however, be interesting to see how this case evolves.

There is also a controversial and "fuzzy" new law that has been introduced by the UK government, and I'm not sure this has been well thought out at all. Section 76 of the Counter Terrorism Act is intended to stop photographs being taken of officers participating in counter terrorist operations. Few would argue that this is a good thing. However, taken in its broader context, any officer could challenge a photographer. Essentially, Section 76 means taking a photo of a police officer (or member of the armed forces), depending on how the situation is judged at that moment, could give rise to your arrest. Civil liberty groups and media unions are up in arms about the law, but protecting the identity of personnel involved with this difficult work is vital. It is all about context, and senior officers have already played down the furore.



THE GCHQ WHISTLEBLOWER

The story of Katherine Gun, the GCHQ whistleblower who was arrested and charged for breaching the Official Secrets Act in 2004, is now featured in a new book *'The Spy Who Tried to Stop a War'*, by Marcia and Thomas Mitchell. Gun, a low-grade intelligence officer (translator), leaked an official US intelligence e-mail concerning espionage at the United Nations. This, around the time the US and UK were seeking support for direct action against Saddam Hussein.

That leak caused an absolute firestorm in Downing Street, but Gun said she acted to help stop war, even though she knew she was breaking her secrecy oath. However, despite the story being major news

in the UK, hardly any of the American media covered it. "I did it with a clear conscience hoping to prevent the war," Gun said in subsequent interviews. "I have no regrets and I would do it again."

GCHQ sacked her shortly after the story broke.

Besides the book, Eye Spy has learned that Gun's spy adventures - bugs, espionage and political drama et. al. is being made into a movie. The screenplay has already been written by Sara and Greg Bernstein.



MONEY FEARS AND TERRORISM

New US intelligence chief warns global meltdown will result in increased terrorist activity despite "weakened al-Qaida"

Dennis Blair, President Obama's new Director of National Intelligence, has warned the global economic meltdown could be the catalyst for increased terrorism. "The primary near-term security concern of the United States is the global economic crisis and its geopolitical implications," Mr Blair told a senate panel. "Economic crises increase the risk of regime-threatening instability if they persist over a one to two year period."

Speaking on a wide range of intelligence issues, Mr Blair said



Mike McConnell

that although al-Qaida's leadership had been weakened by the ongoing security offensive in Pakistan and Afghanistan, the terror group is still capable (and planning) to attack the United States. He also cited Europe as a "launch platform" for an envisaged attack.

The border region between Pakistan and Afghanistan was mentioned as a key element in preventing the terror group mounting attacks beyond this region. The intelligence commentary, probably provided for by information assessments from the CIA, notes that terrorist groups in the region will launch more attacks like that seen in Mumbai and Islamabad. The intention being to provoke an all-out war between Pakistan and India. Indeed, Pakistan intelligence has recently advised its own government, that the Taliban is intent on governing the entire country.

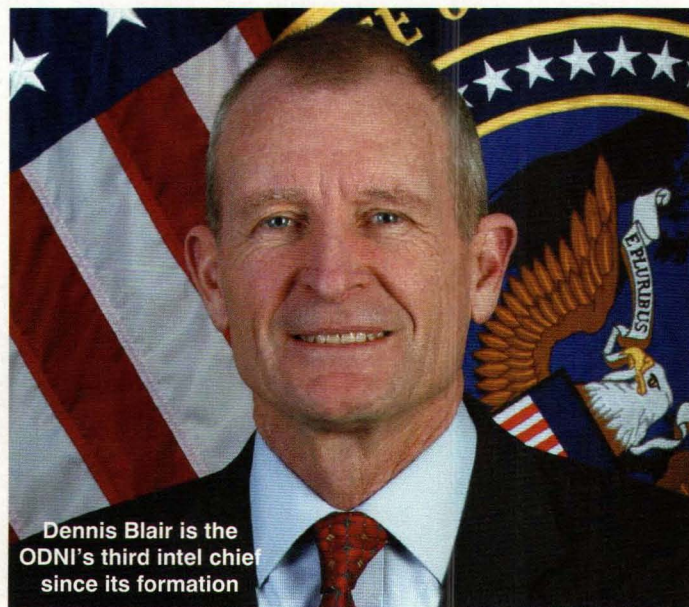
Mr Blair warned the terror group is gaining a formidable foothold in Kenya and Somalia, and warned

attacks planned in these countries would increase and impact against the West.

Besides al-Qaida, Mr Blair commented on the "Iran factor". President Obama believes dialogue with Tehran is vital in securing a peaceful conclusion to its nuclear programme, but Mr Blair notes that Iran, at the very

least, "is keeping its nuclear option open."

Mr Blair is the third person to occupy the relatively new post, taking over from John Mike McConnell. The Office of the Director of National Intelligence coordinates the activities of all sixteen primary US intelligence and security agencies.



Dennis Blair is the ODNI's third intel chief since its formation

ANALYSIS

ODNI versus CIA

Tensions, communications and 'trench lines' await new D/CIA

The Office of Director National Intelligence (ODNI) was created as a direct result of the attacks on America in 2001. Prior to the ODNI, it was the Central Intelligence Agency that wore the "signature stripe" as the country's leading intelligence agency. The head of the CIA not only looked after his agency, but as DCI (Director Central Intelligence) he had a pivotal secondary role in engaging with all of the US services. When the DNI came along, much of his power was perceived to have disappeared, despite claims to the contrary. This has inevitably led to tension.

The ODNI has been likened to a central reporting and coordinating (of intelligence) office with threads to all sixteen US agencies. And there has always been rumours that the CIA and ODNI don't always see eye-to-eye. Outgoing CIA chief, Mike Hayden, a former head of the NSA, believes that whilst tension does exist, it is not always a bad thing. Commenting on the ODNI he said: "Americans being Americans, they're going to fill up their day trying to doing something impactful... which means between the two of us there's going to be a trench line out there."

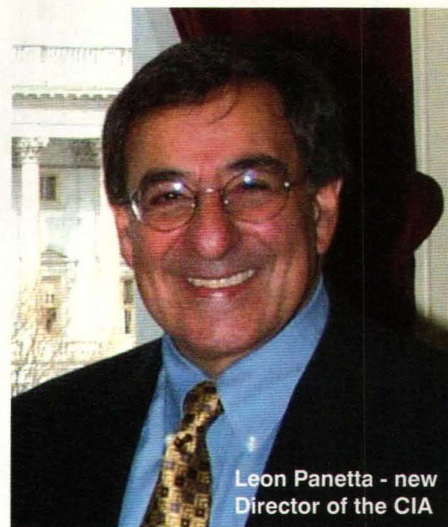
Outgoing DNI, Mike McConnell responded to these words by saying: "Anytime you have



organisations that have similar interests, you're going to have disputes. And particularly if the two leaders aren't working together and having a partnership and so on, the warfare at the trench level gets to be pretty much a raging battle."

New DNI Dennis Blair has another Obama man to work with at the CIA, Leon Panetta. President Obama's choice for D/CIA has not gone down well at Langley, with past officials noting he has absolutely no intelligence experience. Strangely, this may have been evident during his confirmation hearing. Mr Panetta appeared not to understand the relationship between the CIA and the ODNI. He was asked if he would be under the DNI. Mr Panetta told journalists: "We are an operational arm, just like the [NSA, just like the [NRO], and I believe the role of the DNI is to coordinate all our activities..."

A US politician was a little bemused by these comments, and asked Mr Panetta: "Is the DNI



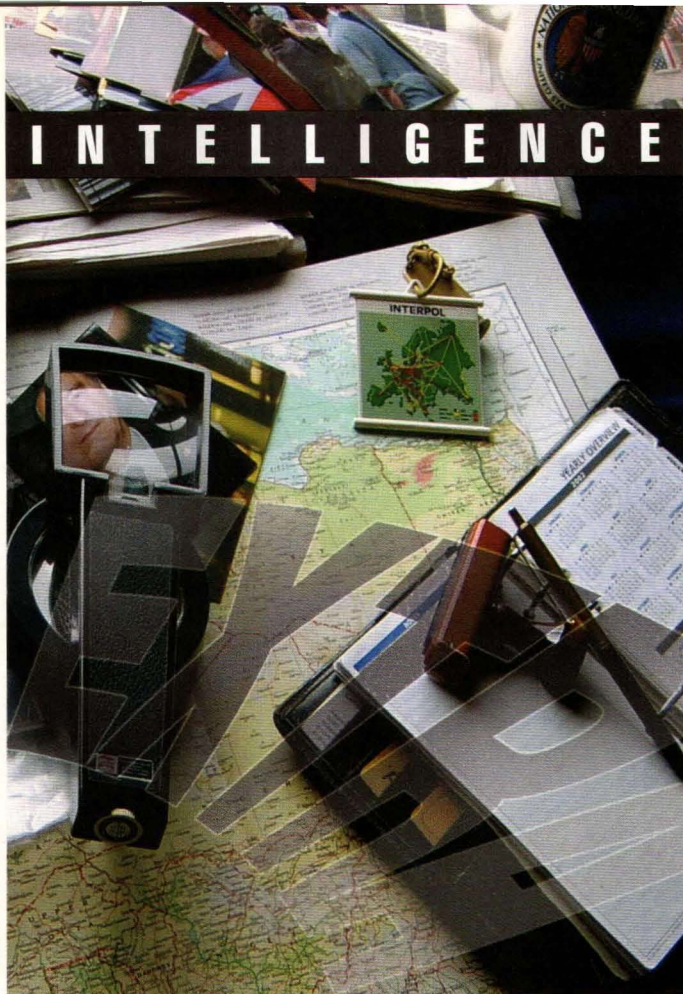
Leon Panetta - new Director of the CIA

your boss or not?" Mr Panetta answered: "The DNI is my boss."

It's certainly not that simple as some agencies report elsewhere and the ODNI does not coordinate CIA operations and the running of the agency. This comment is plainly wrong. As for the CIA chief being under the DNI, that's a blurring of the lines as well. It's our understanding the Director of the CIA reports to the DNI, as do other intel chiefs. Similarly, he can also request assistance for operations.

The ODNI is a vitally important, though complex body that receives, coordinates where necessary, and distributes intelligence to all of the US intelligence elements. Within its mechanism it also has the capability to support the Intelligence Community (IC) liaison, store data, analyse and research. It is not, as we understand, an instructional or operational entity. The DNI ultimately reports to the President and Congress.





SYRIAN NUCLEAR CHASE

Inspectors find graphite and uranium

Despite intensive efforts by Syrian military contractors to remove all evidence of a destroyed nuclear factory, IAEA inspectors confirmed they have found traces of graphite and uranium. Israeli warplanes bombed the well-advanced site in the Deir ez-Zor region in September 2007. This, after satellite imagery and intelligence gleaned by an on-site Mossad agent, confirmed the factory was a nuclear reactor - almost certainly connected to Iran's ambitions. The new findings, described by the UN as "significant", are evidence the site was indeed a covert graphite nuclear reactor. In November, an early IAEA report said that the imagery bore features to an undeclared nuclear reactor.

MI6 and other overseas intelligence collection agencies were thereafter given evidence by Israel that the factory was being built to specifications provided for by North Korea. Ultimately it was designed to produce plutonium for atomic bombs.



NEW 'DIRTY WAR'

The Mossad brings out its bag of tricks

According to a former CIA officer, Israel's "policy" towards Iran has changed from simply gathering intelligence on its nuclear ambitions, to one of a *dirty war* - using all the shadowy tactics perfected by the Mossad.

Since 2005, intelligence watchers have suggested Tel Aviv was gearing up for a multi-strike operation against all of Iran's nuclear sites. All the evidence pointed towards that goal, including at least two "dummy" air attack exercises, one of which reached the shores of Italy. However, the dynamics changed in late 2008, this when President Obama won the race for the White House. Now with increasingly "friendly overtones" from Washington to Iran, Israel has embarked upon a disruption plan that is intended to wreak havoc on its nuclear personnel. Few people doubt the Mossad's capability in infiltration, but the CIA source, speaking to Britain's *Daily Tel-*

graph, said the country has launched what is in effect, a dirty covert war, with the primary intention of slowing down Iran's charge towards the bomb.

At the forefront of Israel's secondary plan, is the alleged intention to "remove" key Iranian nuclear technicians and the outing of companies providing technical support. The CIA man said: "Disruption is designed to slow progress on the programme, done in such a way that they don't realise what's happening. You are never going to stop it. The goal is delay, delay, delay until you can come up with some other solution or approach. We certainly don't want the current Iranian government to have those weapons. It's a good policy, short of taking them out militarily, which probably carries unacceptable risks."

The "long arm" of the Mossad may already have begun its OSS-SOE-type warfare. The intelligence service was allegedly behind the

strange death of Ardeschire Hassanpour. He was one of Tehran's senior nuclear scientists based at the country's Isfahan uranium plant. He died of poisoning from a mysterious gas on 16 January 2007.

An Eye Spy source in Tel Aviv said much disinformation about Israel's intention towards Tehran's nuclear programme is being spread. "The disruption and assassination scenarios are always available and will keep Iran guessing."

Meanwhile, sceptics who dismissed Iran's race towards a nuclear device were shocked when investigators from the IAEA (International Atomic Energy Agency), revealed they had logged an additional 209 kilograms of low-enriched uranium - previously undisclosed by Iran.

Nuclear experts say this discovery now takes Tehran over the threshold of "nuclear breakout capability". Essentially, Iran can build a small nuclear bomb in one year.



© HAMED SABER

SEAR'S TOWER PLOT

Third US trial for alleged terrorists

The third trial of members of an alleged US al-Qaida terror cell has begun. The Miami-based men are accused of plotting to destroy Chicago's Sears Tower and bomb FBI offices. A federal prosecutor said they had "sold out their country for money."

Ana Jhones, said the FBI had created a sting operation, and the agency had lured the men with promises of money. "This case is a 100 percent setup, this is a manufactured crime," said Jhones.

Dubbed the 'Liberty City Six' the men have previously testified they

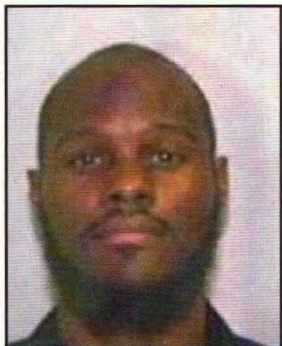


LIBERTY CITY SIX - The group were named after their hometown of Liberty City, an area of greater Miami

An FBI operative infiltrated the gang and gathered intelligence on the men - all had sworn an oath of allegiance to Osama bin-Laden. The agent had secured the men's trust and posed as a terrorist fixer and financier. The gang was headed by Narseal Batiste, 34. His solicitor,

were never serious about the plot. Batiste was only interest in getting his hands on \$50,000.

They were arrested in 2006, and though no evidence has emerged that the plot progressed any further than in the minds of the men, prosecutors say what's relevant is their intention. "It's what they wanted to do," said Assistant US Attorney Jacqueline Arango.



'Cell' leader - Narseal Batiste

Much evidence has been gathered on the gang's surveilling of targets. Besides the iconic Sear's Tower, the men took photographs of an FBI building, a courthouse complex and a synagogue.

• Two previous trials ended in hung juries.

Iran gun placement protecting the Natanz nuclear site



AUSTRALIAN SPYMASTER TO SPYCATCHER

CANBERRA: **DAVID IRVINE**, director-general of the Australian Secret Intelligence Service (ASIS), the country's foreign spy agency, is front-runner in the race to head the Australian Security Intelligence Organisation (ASIO). ASIO's current director, Paul O'Sullivan, a former foreign affairs adviser to John Howard, is to take up the job of high commissioner to New Zealand. ASIO's tasks include counter-espionage and counter-terrorism. Mr Irvine, 62, has headed ASIS since 2003.



David Irvine

MUMBAI LINKS BY WAY OF TELEPHONE CALLS

LONDON: There were "indirect connections" between the terrorists who attacked Mumbai in November and individuals in Britain, the head of MI5 explained in a major interview with the British media. MI5 director **JONATHAN EVANS** explained that billing records have been uncovered revealing telephone calls between the Pakistan-based Lashkar-e-Taiba group suspected of being behind the Mumbai attacks and other countries.

THE ERGENEKON

ANKARA: The NSA's **LT. GENERAL KEITH ALEXANDER** visited Turkey in February and met with the country's General Staff. Media speculation about the scheduled meeting was intense. Some journalists believed military officials discussed the on-going fight with al-Qaida elements, the outlawed Kurdistan Workers' Party (PKK) and general intelligence issues. However, sources say that a more controversial issue was also on the agenda - and one connected to a possible Turkish wiretap operation. For some months the press in Turkey have reported on a shadowy "network" of military, civilian and criminal people - known as the 'Ergenekon'. A court case concerning some alleged members is ongoing and has caused concern because tape recordings have found their way onto the Internet. These allegedly reveal senior military figures admitting their involvement in criminal activities.



Lt. General Keith Alexander

WIRETAP AGENCY LOSES CONTROL

BOGOTA: Colombia's domestic intelligence service - the Department of Security (DAS), is embroiled in a bitter row over allegations that it secretly wiretapped judges, politicians and journalists. Defence minister Juan Santos said he discovered his own conversations, along with his 12 closest ministers were recorded. DAS's deputy of intelligence, Captain **JORGE LAGOS**, has already resigned over the operation. Meanwhile, Colombia's President Uribe has said wiretap operations will be placed under the control of the National Police... itself accused of illegally listening-in on phone conversations.



Head of DAS Felipe Munoz

PERSONA NON GRATA

QUITO: Ecuador's President Rafael Correa, has accused a US diplomat of conducting CIA operations in his country. Mark Sullivan, the US Embassy's First Secretary was declared a "persona non grata" - a polite term often used when persons are expelled from a state... usually for spying. Correa accused Mr Sullivan of being the CIA's Station Chief, but he offered no evidence for any of his "spying" accusations.



OPEN SOURCE



Former KGB spy buys into UK media

Former KGB officer Alexander Lebedev, 49, has purchased one of the UK's most important and long-running newspapers. Lebedev, a billionaire businessman, bought around 75% of the London Evening Standard newspaper for just £1. The paper, which has a circulation of just under 300,000, passed into the hands of the Evening Press, a company formed by Mr Lebedev and his London-based son Evgeny Lebedev, 28, and owned by Lebedev Holdings.

Critics and intelligence watchers greeted the purchase with much suspicion, but Lebedev said he is a strong believer in a free press and "would not interfere with the paper editorially." Sir Peregrine Worsthorne, former editor of The Sunday Telegraph, said the take-over was a sign of "national decline".

The capture of this famous title comes at a time when London is experiencing a city-wide "free newspaper war", and the Evening Standard was losing much valuable revenue.

Lebedev, who coincidentally used the Evening Standard to gather intelligence (open source) when he was operating as a KGB spy in London, has his eyes firmly set on other newspapers, including at least two well-known titles in the United States.

Others have warned that Lebedev's purchase could set a precedent for other wealthy

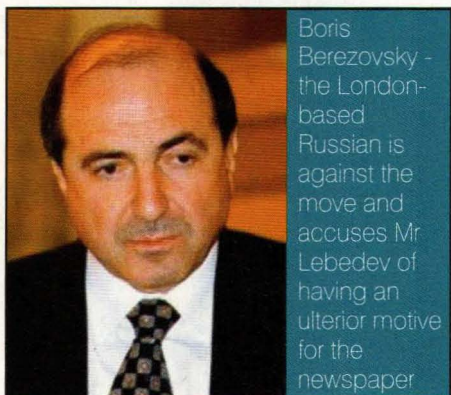
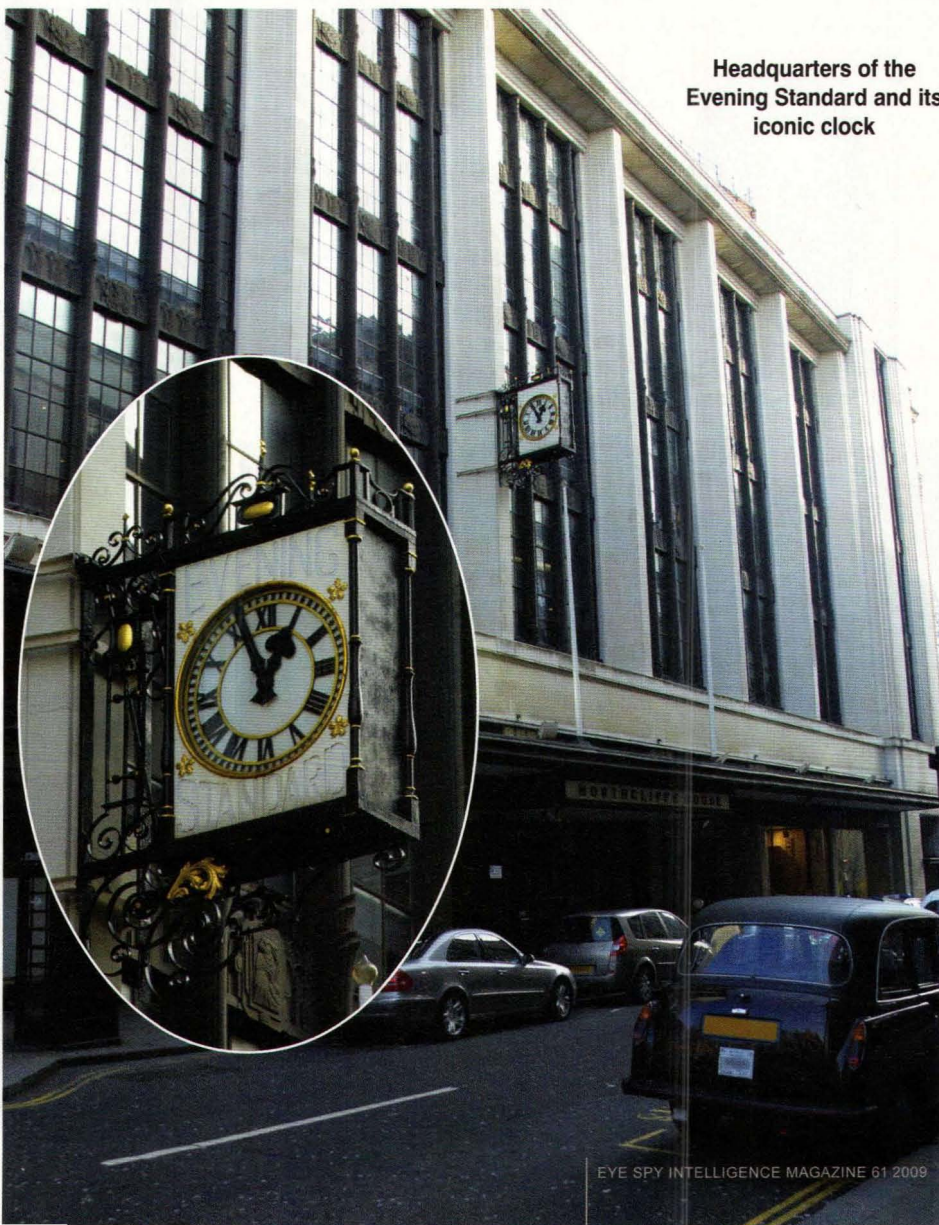


Alexander Lebedev and former President Vladimir Putin pictured in 2002

Russians buying media abroad, including exile Boris Berezovsky, who is wanted for extradition by Moscow.

Journalist Roy Greenslade, who writes a column in The Standard, was asked why Lebedev purchased the paper. "What you always have to ask yourself is, 'Why is this person buying the paper?'" Mr Greenslade said. "There are five reasons for owning newspapers, and all begin with a P: profit,

Headquarters of the Evening Standard and its iconic clock



Boris Berezovsky - the London-based Russian is against the move and accuses Mr Lebedev of having an ulterior motive for the newspaper

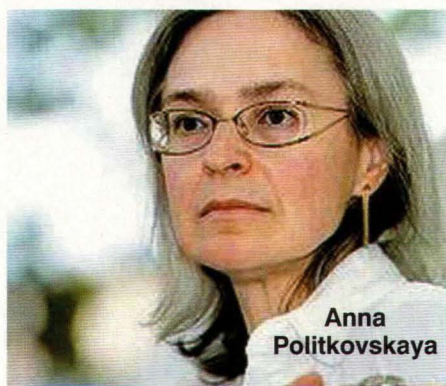


Yury Fedotov

Yury Fedotov, Russian Ambassador to the UK, dismissed Berezovsky's claims: "Mr Berezovsky is wanted for criminal cases of embezzlement and money laundering... so he knows about dirty money, he knows about money laundering, so he's an expert in these matters. I wonder why he continues to enjoy the status of political exile."

Back in Moscow, Mr Lebedev, who is believed to have a \$3 billion fortune, is the major shareholder, along with the former Soviet president Mikhail S. Gorbachev, in Novaya Gazeta. This independent title has often run features on press and government freedom and generally supports democracy. One of its well known journalists was Anna Politkovskaya, a friend of the murdered former FSB officer Aleksander Litvinenko who was gunned down in Moscow in October 2006.

On 26 January this year, Anastasia Baburova, a freelance journalist for Novaya Gazeta was also killed in Moscow. She became the fourth Novaya Gazeta journalist to be killed since 2000 (see sidebar).



Anna Politkovskaya

propaganda, political influence, prestige and public service. There's no profit in The Standard, so you've got to look at the other things."

Berezovsky launched into a vociferous attack on learning of the newspaper purchase, accusing Moscow of using its wider "assets" to influence political and media outlets. "Putin and his cronies have made absolutely dirty money and tried to invest this money all over the world including Britain," he said. He believes the Evening Standard will become a "propaganda vehicle" for the Kremlin. "Lebedev will try to spread information that will help Russian authorities to survive without understanding it is not possible in this country at all."



Founded in 2002, Autonomous Action has been described as a "revolutionary anarchist federation." Intelligence watchers say it is comprised of anarcho-communists, syndicalists, autonomist-Marxists, and radical ecologists. Anastasia Baburova was reportedly a member of the group which operates mostly in Russia, Ukraine and Belarus

UNDERWORLD

A familiar ending in Moscow

Ukrainian-born Anastasia Eduardivna Baburova was a trainee journalist at Novaya Gazeta and a student of journalism at Moscow State University. As a member of 'Autonomous Action' she often found herself investigating cases relating to human rights and civil liberties. She was shot dead in Moscow on 19 January 2009, along with human rights lawyer Stanislav Markelov. Russian police believe it was Markelov who was the real target.

When a masked gunman confronted Markelov, and ultimately shot him, Baburova reportedly tried to intervene. She was killed with a single shot to the back of her head.

Markelov, a fairly prominent lawyer in the city, had worked on numerous high-profile human rights cases. But he is better known for the case involving Elza Kungayeva - a Chechen woman killed by Colonel Yuri Budanov, a Russian Army officer in 2000. After learning a Russian court had granted Budanov an early release, Markelov urged the court to change its mind. Two weeks after Markelov and Baburova were assassinated, Budanov was set free.



Stanislav Markelov and Anastasia Baburova - shot by a professional gunman

THE UNIDENTIFIED RUSSIAN ASSASSIN

In June 2007, New Scotland Yard foiled a plot to assassinate the exiled Russian tycoon Boris Berezovsky.

The gunman was surveilled from the moment he entered Britain via Heathrow Airport. He had arranged to meet Mr Berezovsky at the London Hilton Hotel. However, Berezovsky's own intelligence people had secretly flown him out of the country, unbeknown to the gunman, who was duly arrested by police on 21 June.

The affair was quietly played down and police handed the would-be assassin, who used his son as a decoy, to the immigration services two days later. (See Eye Spy 50 for further details)



A EUROPEAN CONNECTION?



Intricate operation launched against Mumbai was "part planned" in Pakistan but has threads to European and other global terror networks



MUMBAI

Pakistan's Inter Services Intelligence Agency (ISI), has confirmed the terrorist operation in India's financial capital, was "part planned" in Pakistan, and that nearly all those involved were its own citizens. This, after India forwarded a huge dossier to Islamabad on 5 January which contained the results of its preliminary investigations. However, several intelligence agencies, including MI5, are still probing links to suspects in Europe.

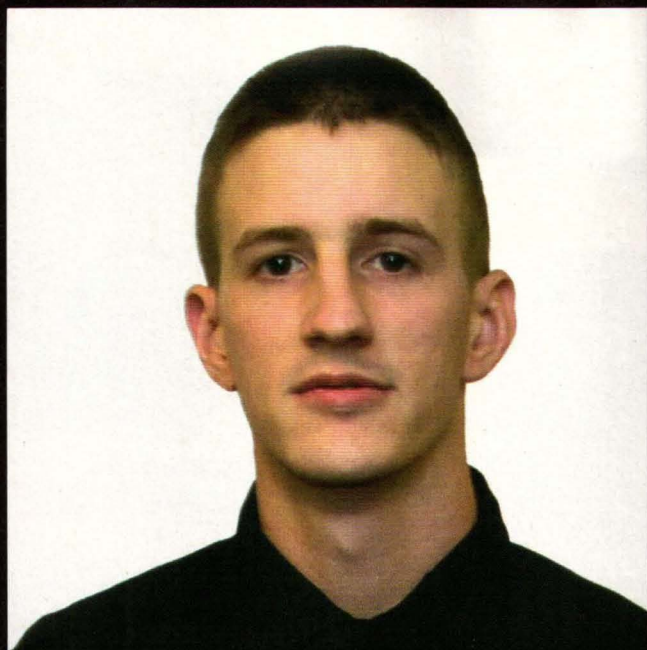
Some eight people have been arrested in various towns and cities across Pakistan, following a detailed investigation supported by officials from the FBI and other agencies. Two of those in detention are considered "senior

plot masterminds" - Zakiur Rehman Lakhvi and his operations' and communications' commander - Zarar Shah. The lead operational facilitator has also been named as 38-year-old Hamad Amin Sadiq, from the Punjab province, while two men identified as "Khan" and "Riaz", are accused of coordinating the attacks. All are believed to belong to the Lashkar-e-Taiba (LeT)*. Two other men connected to the support element of the attack are being sought.

Various intelligence and clues led to the arrests, including the tracing of cell phone calls made by the attackers to the gang's Pakistan-based headquarters and other operatives' cell phones. Dozens of calls were identified by communications experts, some

of which were not received, presumably when the attackers were killed. The forensic cell phone number trail also led to Spain and Italy and two suspected senior members of the terror cell. According to the ISI, Mohammad Ashfaq and Javed Iqbal, who lived in Barcelona, used the Internet to control parts of the operation and remain in contact with the attackers.

Other countries are also linked to the plot. For example, one of the Sim cards retrieved by Indian police actually originated in Austria. A sum of \$238.00 was wire-transferred from a location in Spain to establish a domain name, this being necessary for the operatives to communicate and pass messages to each other in secret. The domain name was actually



OBRYANT

The dangers of serving abroad in a region laced with several organised terrorist gangs was emphasised in the bombing of the Islamabad Marriot Hotel on 20 September 2008. Amongst the 266 fatalities was US Cryptologic Technician 3rd Class Matthew J. O'Bryant, 22. The liaison officer was assigned to the Navy Information Operations Command in Fort Meade.

registered in Houston, Texas, and payment made in Italy. The system allowed for "teleconferencing" which is almost impossible to intercept. Javed Iqbal, who used three separate e-mail accounts, has been linked to the original transaction for the Voice Over Internet Protocol (VOIP). Another domain name used by the gang was registered in Russia. Of further interest, a Thuraya satellite phone connected to the terrorists

A US Navy security detail swoops on a suspected Somali pirate "fast boat". The Mumbai terrorists were clearly schooled in the use of such vessels and inflatable dinghies and used them to great effect. Right: A Thuraya satellite phone was recovered from one of the gang's primary boats. The device kept operatives in touch with their colleagues back in Pakistan, and helped them navigate the waters.



Overhead view of the sprawling Port of Karachi

ZAKIUR REHMAN LAKHVI - THE JOURNEYMAN



Indian officials examine the devastation caused by the terror attacks attributed to Lakhvi and his associates in 2006



Zakiur Rehman Lakhvi, aged around 50, is regarded as one of the founding members of the Lashkar-e-Taiba terror outfit and sits on its so-called 'General Council'.

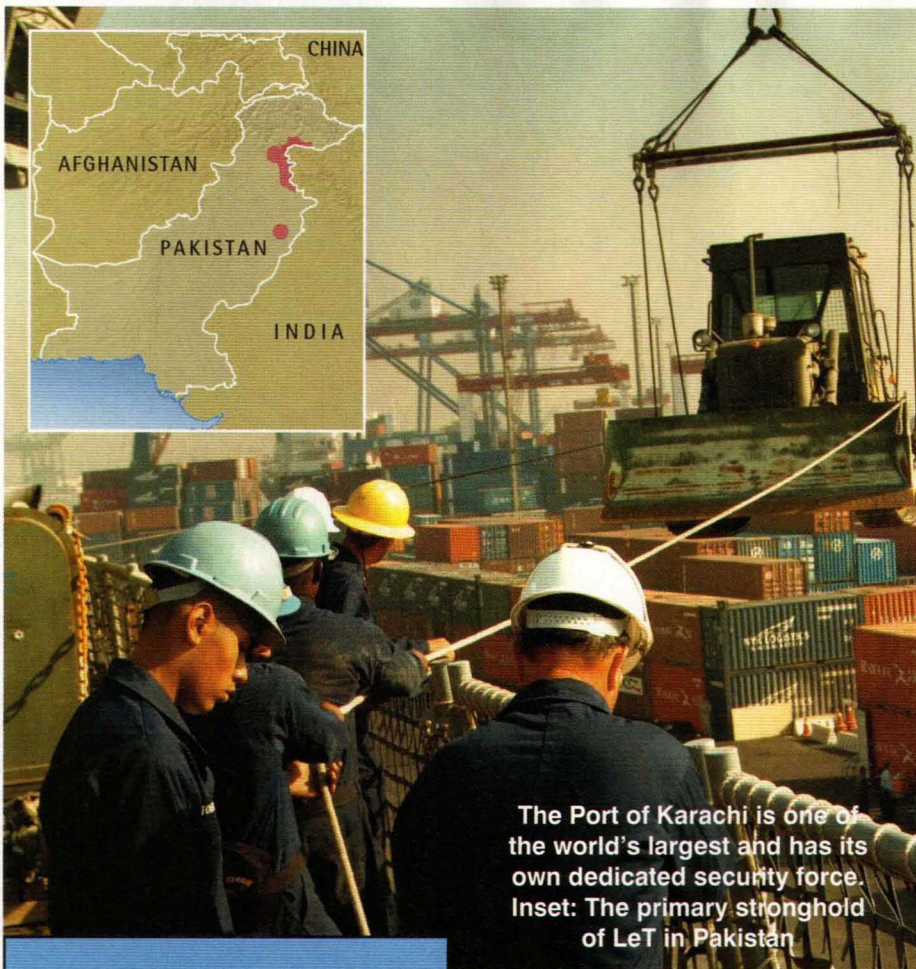
CIA analysis states he has operated in various theatres including Chechnya, Bosnia and probably Iraq. In previous 'media releases', he has openly said targets in India would be attacked.

Lakhvi is connected to the devastating raids on the Mumbai rail network on 11 July 2006, by his association with Azam Cheema, one of the senior figures suspected of planning the operation. Some 200 people died and a further 500 were injured.

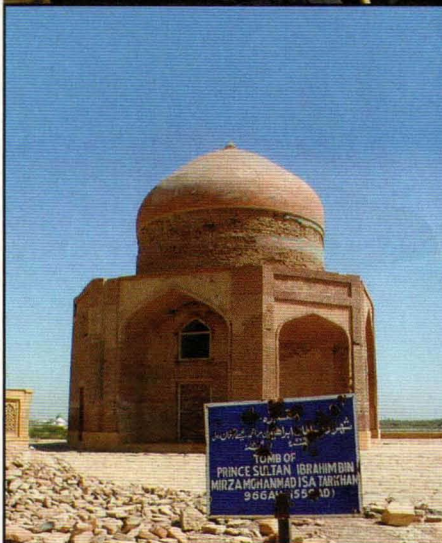
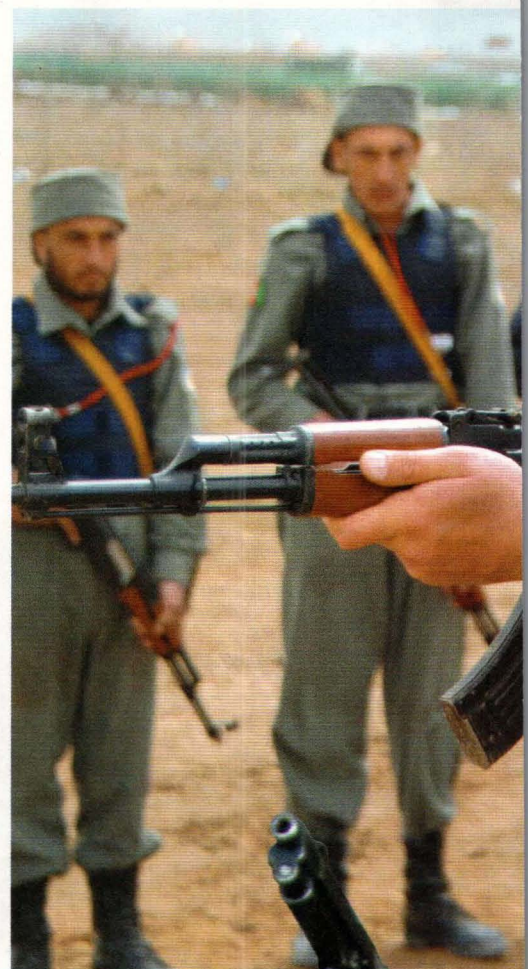
Lakhvi was arrested on 7 December 2008, at an LeT training camp. Earlier that year in May, the US Treasury Department froze assets reportedly linked to Lakhvi.



COURTESY: US NAVY



The Port of Karachi is one of the world's largest and has its own dedicated security force. Inset: The primary stronghold of LeT in Pakistan



was registered in a Middle Eastern country, and according to the ISI, was purchased by a "non-Pakistan citizen". This country has not been named. The phone was found aboard the *Kuber*, a 75ft fishing trawler floating near Mumbai. Its captain, Amar Narayan, was found with his throat cut. Investigators also probed the payments made to the actual operatives involved in the attacks - these monies also originated from Italy. It has also since transpired, that the terrorists left the Port of Karachi aboard a vessel called the *Al Hussaini*, and almost certainly hijacked the *Kuber* en-route to Mumbai. Authorities in the region have yet to find this boat, though Pakistan maritime police issued a statement on 12 February 2009, saying it had sunk shortly after the attack.

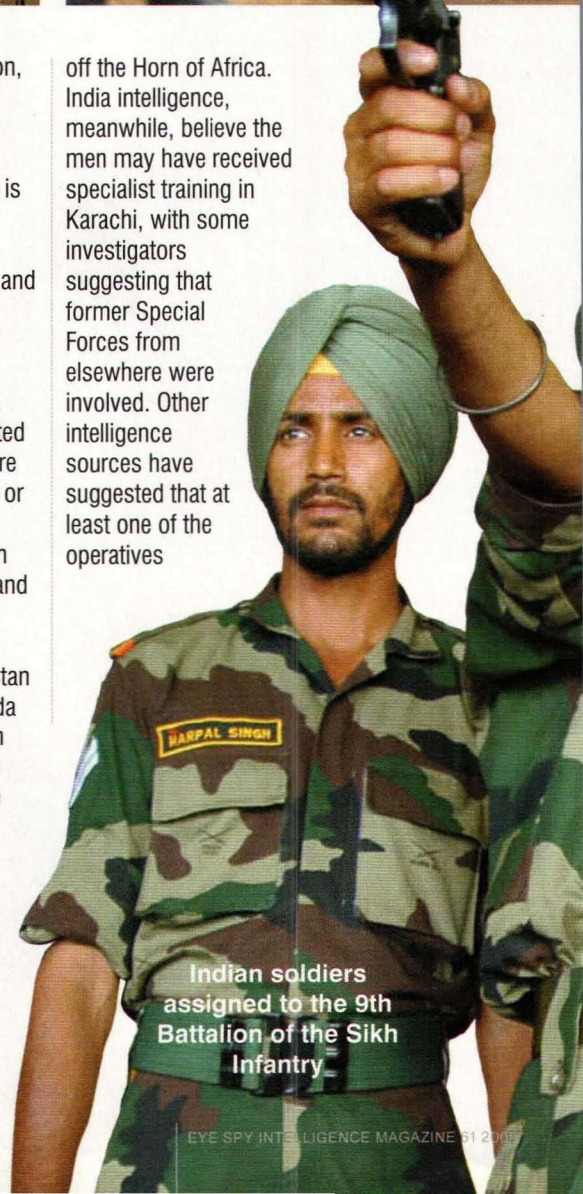
In respect of a possible Austrian connection, its Foreign Office denied any part of the Mumbai operation was planned there.

Nevertheless, US intelligence believes this is an indication just how widespread and complex the planning of Mumbai was. Officials from Interpol, New Scotland Yard and the FBI are all involved in what is, a truly global investigation.

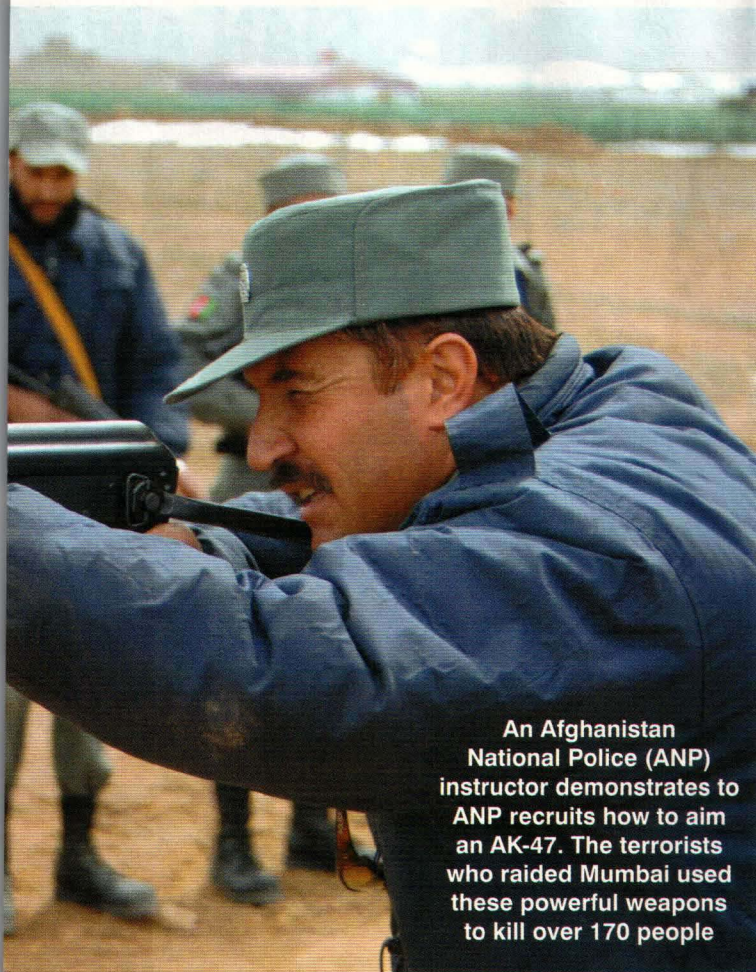
Pakistan's Interior Minister, Rehman Malik, explained that the terror cell's planners opted to use two safehouses - both of which were active at the height of the operation. Three or four boats that carried the operatives to a waiting vessel have been traced to Pakistan ports, this after a boat engine was seized and its number identified.

ISI officials say the ten attackers - all Pakistan nationals and likely members of the al-Qaida franchise group - Lashkar-e-Taiba, sailed in three boats from the port of Karachi, in the province of Sindh, and then refuelled in the Indian state of Gujarat. The gang had travelled to the port from the nearby historic city of Thatta, probably to avoid the Port Security Service which has a major presence on site. It is understood US satellite surveillance tracking records have confirmed this. On nearing Mumbai, they transferred to a high-speed boat similar to craft used by Somali pirates

off the Horn of Africa. India intelligence, meanwhile, believe the men may have received specialist training in Karachi, with some investigators suggesting that former Special Forces from elsewhere were involved. Other intelligence sources have suggested that at least one of the operatives



Indian soldiers assigned to the 9th Battalion of the Sikh Infantry



An Afghanistan National Police (ANP) instructor demonstrates to ANP recruits how to aim an AK-47. The terrorists who raided Mumbai used these powerful weapons to kill over 170 people

was himself a former member of an "external armed force." The ISI also say that while most of the "components" for the attack were purchased in Karachi, including the powerful AK-47 assault rifles, there is a definite connection to "elements" in Europe.

Eye Spy has learned that investigators are still researching "credible evidence" that a "second wave" was planned by terrorists, this almost certainly related to the hijacking of an airliner - the objective being likened to what happened in New York in 2001. This relates to a number of e-mails sent by an associated terrorist group. We also understand that the training manual and plot details of Mumbai have been circulated to other terrorist cells, and may have already been used as early as 10 February 2009, in Kabul, Afghanistan. US and British intelligence are examining a daring Taliban raid on government offices in the city that left over 20 people dead and dozens more injured.

Though the ISI is being seen to be acting aggressively against those involved in the case, it didn't stop Indian Foreign Secretary Shivshankar Menon from accusing the spy agency of "direct involvement." This has been strenuously denied by government officials in Islamabad. Pakistan, while acknowledging "part of the plot" was devised by its own nationals, have argued that the case is one of global significance and should be investigated by the international security community.

Those arrested in the recent Pakistan raids, have been charged with "aiding and abetting, conspiracy and facilitation" of a terrorist act.

* Lashkar-e-Taiba translates to Army of the Righteous

SURVEILLANCE

HIGH-QUALITY REAR VISION SURVEILLANCE SUNGLASSES



**USED ONLY
BY PROFESSIONALS**

Eye Spy Intelligence Magazine rear-vision surveillance sunglasses have a black-metal designer frame, rubber-backed ear drop-over (for comfort) and superb glass lenses. They also come in a tough smart black carry case. Don't confuse these glasses with other cheap models that are easily spotted, or others that carry the Eye Spy name. The reflective mirror in our glasses is actually embedded into the lens and impossible to detect



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

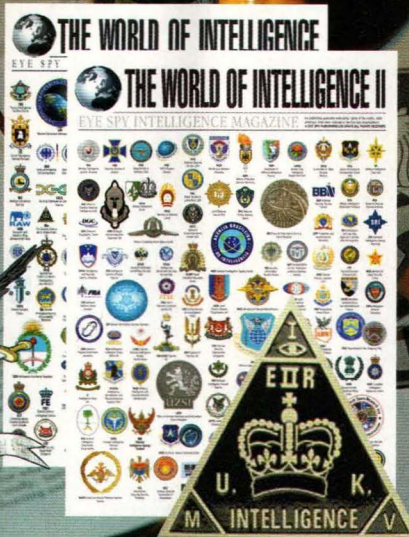
FOR 2009

FANTASTIC VALUE!

GIVE AN

EYE SPY

GIFT SUBSCRIPTION



AN EYE SPY GIFT SUBSCRIPTION INCLUDES INTEL CRESTS POSTERS 1 AND 2, OUR INTEL MOUSE MAT AND A BINDER! CALL FOR DETAILS OR VISIT www.eyespymag.com (subscription section)

RUSSIAN AND A SPY KEEPIN

QUALITY EYE SPY BINDERS

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



Order Ref:

ES/099

UK £7.50

USA \$17.00

ROW £9.50 -

price includes P & P



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



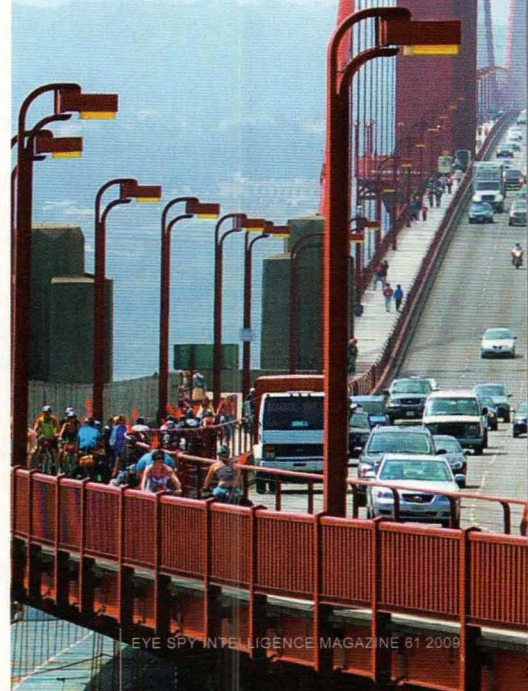
Eye Spy's brilliant 'Intelligence Services of the World' mouse mat features some of the most famous intelligence crests in the world.

Provides superb mouse control and razor-sharp quality, this full colour mouse mat will be a talking point in office and home! (Optical friendly)

INTELLIGENCE SERVICES OF THE WORLD MOUSE MAT

Ref: ES/MM UK £7.99 USA \$17.00 WORLD £9.50 (price includes postage and packing)

WITH SUBSCRIPTION CARD UK £6.99 USA \$15.00 ROW £8.50



AMERICAN

GAMES



IT IN THE FAMILY

A former CIA officer and double agent has appeared in court alongside his son. They are charged with a number of offences... including liaising and imparting information to Russian intelligence....

A senior CIA officer jailed in 1997 for spying on behalf of Russian intelligence, tried to run a second spy ring from the confines of his prison cell in Sheridan, Oregon. After Harold J. Nicholson failed to enlist the help of inmates in contacting his former FSB (Russian Federal Intelligence Service) handlers, Nicholson turned to his son Nathaniel for help. However, unbeknown to both men, the FBI were already surveilling the men. This led officers around the world in an effort to glean just what the Nicholsons were planning.

Harold J. Nicholson was no ordinary desk officer or employee. It's understood he was a specialist instructor in the art of spy tradecraft at Camp Peary - the CIA's sprawling 9,000 acre North Virginia training school, better known as 'The Farm'. It is here where field officers and potential recruits are put through their paces and given advanced training in the art of espionage and all of the subject's more shadowy facets. Seeking a little more recompense for his particular skills, Nicholson made contact with the FSB who were only too pleased to give him hundreds of thousands of dollars for the intelligence he would impart.

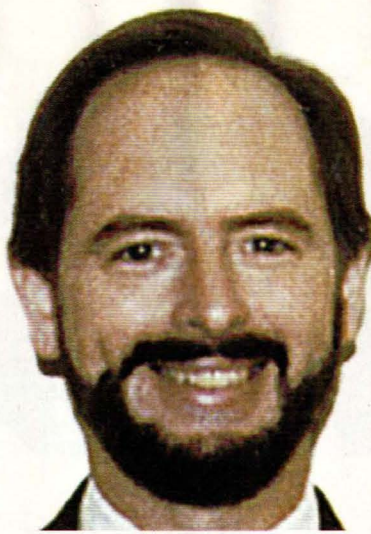
Besides tipping Moscow off about new agents posted overseas - many whom he had helped graduate through the school - he also told his FSB handler the identity of the CIA's Moscow Station Chief in the 1990s. This would undoubtedly have led to a worldwide FSB surveillance operation, noting everyone the SC met with and conversed. It's likely US and UK contacts would have been amongst those "outed".

Nicholson's original plan was to try and make contact with his former spy handler using inmates who were being freed or on parole - this in an attempt to impart more sensitive information (before it was worthless due to its age), but also to obtain a "gratitude fee". The FBI called this a "kind of retirement pension" - reportedly available to him in Russia because of his "honourable service to Moscow". Yet to secure these monies and avoid them being traced, Nicholson had to first make contact, and then conclude the 'contract'. And while this could have been done in America, Nicholson thought it better to liaise overseas - and out of the sight of US intelligence watchers. With his plan to use released prisoners as 'go-betweens' in tatters, Nicholson sought to use the one person he could trust... his son Nathaniel.

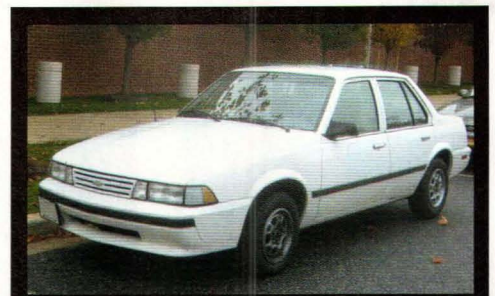
The Golden Gate Bridge in San Francisco. It was here the son of a jailed CIA officer made contact with Russian intelligence



Nathaniel Nicholson



Harold James Nicholson



Nathaniel's Chevrolet Cavalier was fitted with a tracker

'It looks like I will still be able to go on that vacation!... Well hon, I just thought I'd say 'hi' since I had the time!'

Nathaniel, 24, a former US soldier who worked part-time at a tool company and a Pizza Hut restaurant, decided to help his father and allegedly met with Russian intelligence contacts in various cities, including Mexico, Lima and San Francisco - the latter allegedly being the venue for an early 'point of contact'. In early December 2008, undercover counter-espionage FBI agents surveilled Nathaniel to Cyprus. He allegedly met with two FSB officers at a T.G.I. Friday's restaurant on 10 December. Nathaniel, almost certainly acting on guidance provided for by his father, used coded messages and comments to set up the meetings. However, unbeknown to the Nicholsons, the FBI were monitoring his cell phone calls and e-mails - both operations providing valuable intelligence. One puzzling intercept from Nathaniel - who pretended he was writing to his girlfriend 'Nancy' read: *'It looks like I will still be able to go on that vacation!... Well hon, I just thought I'd say 'hi' since I had the time!'* The FBI believe this was confirming the 'contact meeting' on the island.

It is believed Nathaniel was handed \$35,000, which on his return to the United States, was divided into smaller amounts and distributed

between his family - some of it being used to pay for bills. This action was again, allegedly at the behest of his imprisoned father.

OPENING DOORS

The FBI had become suspicious of Nicholson Sr. and his prison activities as early as 2002, after being tipped-off he had asked an inmate to make contact with a former FSB agent on his behalf. One prisoner explained to the FBI how he was asked to deliver a manila envelope to a Russian, whilst another said Nicholson would carefully dispose of all correspondence down the toilet - this after tearing the letters into little strips. FBI counter-espionage agents soon turned their attention to Nathaniel who frequently wrote to his father and then started to visit him in prison. With court approval a tracker was placed on his Chevrolet Cavalier and his apartment in Eugene, Oregon, was similarly monitored.

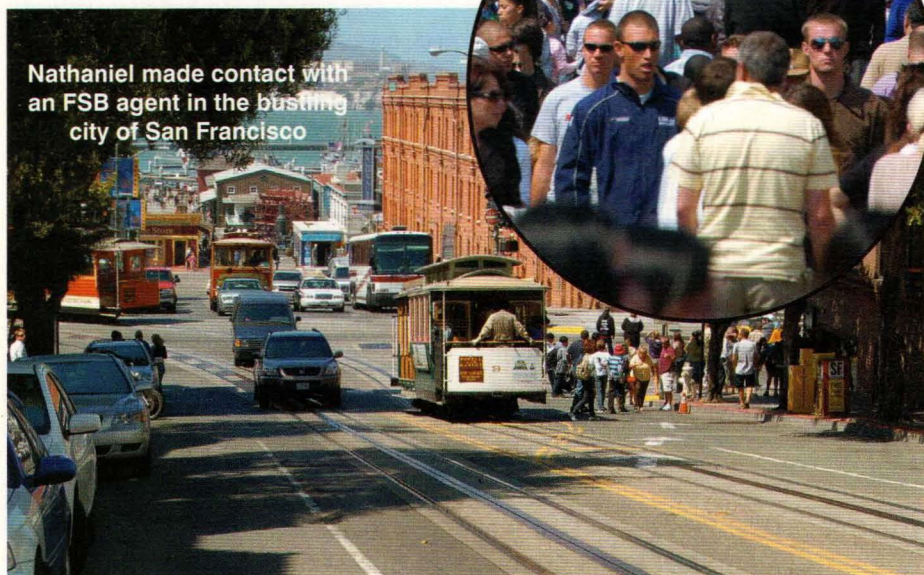
A major breakthrough came in December 2007, when agents surveilled Nathaniel at Houston Airport. As he arrived back from a trip to Lima, Peru, Customs and Border officials ordered a search of him and his luggage. Out of sight of Nathaniel, officials photocopied his notebook and a number of business cards. They also discovered hand-written notes, one of which was the address of the Russian Embassy in Mexico City. FBI analysts began pouring over the notes - and evidence of coded literature reportedly used to liaise with the Russians was instantly recognised. "Friends - Nancy" and "My Name - Dick". Investigators also noted a sentence about his CIA father's arrest that would be of interest to Russian intelligence - "What hints were given showing that the interrogators - knew about the relations before the interrogations?" Another line provided clues that the emerging affair was being kept in the family - "Grandparents know the situation. They are trustworthy, and will help-w/ cover up."

The FSB were very interested to learn how US intelligence had rumbled Nicholson Sr. in the first place. Intelligence gleaned by the FBI revealed that Nathaniel allegedly provided his FSB contact with a family history and the apparent intelligence-based clues that led to their agent being exposed. Nicholson Sr. was detained in 1996 following an undercover operation as he attempted to board a flight to Switzerland. According to a sworn statement by FBI case agent Jared J. Garth, Nicholson Sr. had arranged a meeting with a Russian agent in Zurich.

In another communication between father and son, FBI agents discovered a letter which discussed a new 2008 US law - the 'Second Chance Act'. Nicholson Sr. believed this legislation could be used to lessen his 23-year sentence. According to officials, they suspect the correspondence was meant to reach his former Russian handler who would then be able to arrange for a passport to be acquired.

With a plethora of evidence against the Nicholsons, new criminal charges have been laid against Nicholson Sr. Meanwhile Nathaniel has been charged with conspiracy, money laundering and just as serious - acting as a foreign agent.

US Attorney Karin J. Immergut said the affair was "a sinister and continuing scheme." Both Nicholsons pleaded not guilty in a brief court appearance in late January.



Nathaniel made contact with an FSB agent in the bustling city of San Francisco

The FSB AGENT who believed he was owed a pension for his treachery



Harold James Nicholson was arrested by FBI officers at Dulles International Airport on 16 November 1996, as he was about to board a plane to Switzerland to meet with Russian intelligence officers. On his person were several rolls of film containing images of top secret documents. Within his luggage, detectives found two empty money bags... presumably they would have been used to carry a cash payment back to the USA. At the time, Nicholson had been employed by CIA for 16 years. His top secret security clearance enabled him access to highly sensitive information.

Remarkably, Nicholson embarked on his double agent activities just seven weeks after the conviction of another CIA man - Aldrich Ames - the most notorious spy in CIA history. It was whilst serving in the Philippines, Nicholson was approached by Russian recruiters - but this was an intended covert action by the CIA. The problem was, Nicholson got turned and the CIA were oblivious... for now.

Nicholson worked as an instructor at Camp Peary from 1994 to 1996. It was during this period he forwarded a wide variety of classified US materials, including personal details of

dozens of CIA officers who had trained at the centre to Russian intelligence. Ironically, within the data, passages and transcripts of interviews with Aldrich Ames. Other information imparted to his FSB handler, included the identity of CIA contacts and informants in the wider overseas business community.

The man who once served as Station Chief in Bucharest, even hacked CIA computers and "scooped" huge amounts of intelligence - some of it not even requested - for the Russians. But in October 1995, during his time at the training facility, Nicholson underwent a series of polygraph examinations - some of which he unwittingly tried to beat using methods likened to those used in the former Soviet Union. He failed.

These actions were recognised by CIA polygraph testers and red flags started to fly.

The FBI, in liaison with their counterparts at the CIA, started to cross-reference his meetings in overseas countries with deposits made in his bank. There were many suspicious transactions and liaisons. For example, while in Malaysia, Nicholson held an authorised meeting with officers from Russia's SVR. Twenty-four-hours later, on 30 June 1994, it transpired he had wired a \$12,000 sum into his bank. Officials found several such actions following meetings with the Russians. In total, a little over \$120,000 was deposited, and the FBI could find no adequate explanation from whence this money had come.

Nicholson's spy games continued, but surveillance of his office inside Langley soon provided more evidence that the likable career intelligence officer had been turned. One covert film showed Nicholson photographing CIA documents after removing the classification markings.

Like many spies, this double agent was motivated by greed. During his trial, he claimed the money was to pay mounting debts, a divorce bill, childcare, etc. The court was lenient, despite the fact he had put many fellow officers and undercover operatives in danger. On 3 March 1997, Nicholson pleaded guilty and admitted he was an FSB spy. On 6 June 1997, he was sentenced to 23 years and seven months, though this was because of his cooperation with investigators.

DOUBLE AGENT

CASH FOR AGENT IDENTITIES

Nicholson's spy games came to an end when FBI agents arrested him at Dulles Airport



US intel fears
as watchers
look inwards
as well as
overseas

Eye Spy has learned that two secret American operations have been launched to identify US citizens recruited and trained by terrorists from "home turf". The FBI is investigating over 20 suspected sites (many in remote locations - though not all) in the country where al-Qaida sympathisers are "turning" people to fight in foreign lands. Some of this work is being performed by the Bureau's Joint Terrorism Task Force. However, agents are also monitoring various suspected cells who could one day be persuaded to launch attacks on the US mainland. A number of so-called "settlements" or "camps", are now under observance and are being infiltrated by specialist agents. The CIA, meanwhile, is gathering intelligence on persons who are using Europe as a stepping-stone into the United States - legitimately and without visas -



FBI Director Robert Mueller has warned an attack on a major US city is not beyond the realms of possibility

THE NEW
AMERICAN
SEEK

RECRU
HOME GROW

Visa waiver flights from Europe are becoming a major concern for the FBI and CIA. Both services are of the opinion that terrorists and their recruiters are using Europe as a stepping stone to enter and exit mainland America. According to some sources, they are also liaising with US citizens who have established their own terrorist cells...



on 'e-tickets'. This is one reason why the security services in the UK and USA are keen to create electronic airline logs. Combined with other systems, this will undoubtedly make travel more difficult for those intent on recruitment.

More evidence that al-Qaida is recruiting "vulnerables" on US soil, came last year, when a Somali-American man carried out a suicide bombing in the north of the African country on 28 October. The CIA identified the bomber as Shirwa Ahmed who resided in Minnesota. The FBI fear that more men - some already gathered in "pockets" - may have

been radicalised and are operating abroad, indeed, the CIA have known files on US citizens suspected of carrying out al-Qaida's work in Iraq, Yemen and Afghanistan. The FBI is now trying to trace at least half-a-dozen men from Ahmed's area in Minnesota, also originally from Somalia, who have simply vanished. Analysts are of the opinion some of the men - all in their twenties - may also have been recruited by al-Qaida.

However, it is the security services' fear that an operation like that seen in Mumbai, may well be in the planning via US-based "settlements".

FBI Director Robert Mueller warned that it is not impossible that an attack, similar to the one launched on Mumbai, may well be repeated or tried in one of the big US cities. Mr Mueller said: "How many other cities around the world could fall prey to such an attack? How many cities here, in the United States? It again raises the question of whether a similar attack could happen in Seattle or San Diego, Miami or Manhattan. The attacks were a reminder that extremists with large agendas and little money can use basic weapons to maximise their impact."

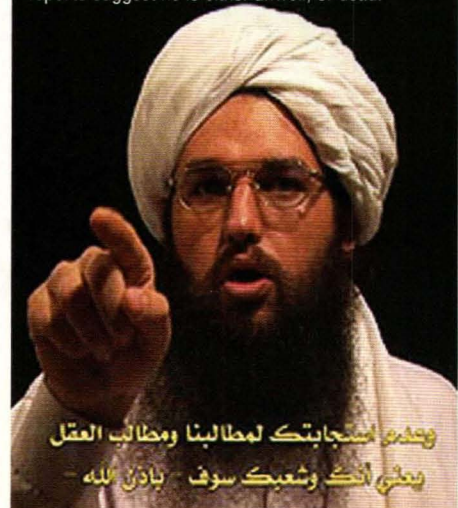
Discussing US citizens, he further warned that the evidence "raises the question of whether

AL-QAIDA'S VIDEO RECRUITER

One of the FBI's most wanted is also an American citizen - Californian Adam Yahye Gadahn. He likes to think he is a prominent member of Osama bin-Laden's inner-circle. Residing in the lawless area that separates Afghanistan with Pakistan, Gadahn is a keen propagandist whose rhetoric is aimed not only at persons willing to help the terror group outside America, but also at those on the mainland.

Using the medium of video and the Internet, Gadahn constantly mocked former President Bush. Such speeches culminated in the US issuing a charge of treason. Not undone by this, Gadahn renounced his citizenship - probably a relief to those in Washington. On film he showed his US passport - ripped it in half and shouted... "Don't get too excited - I don't need it to travel anyway."

Gadahn's undoubted skill in communicating violence - and its justification - led to a \$1m bounty being put on his head. However, he even laughed at this. He is a pivotal component in the terror group's 'media wing' - and has produced numerous broadcasts for As Sahab. Gadahn has made it his mission to recruit people to al-Qaida, though recent reports suggest he is either unwell, or dead.

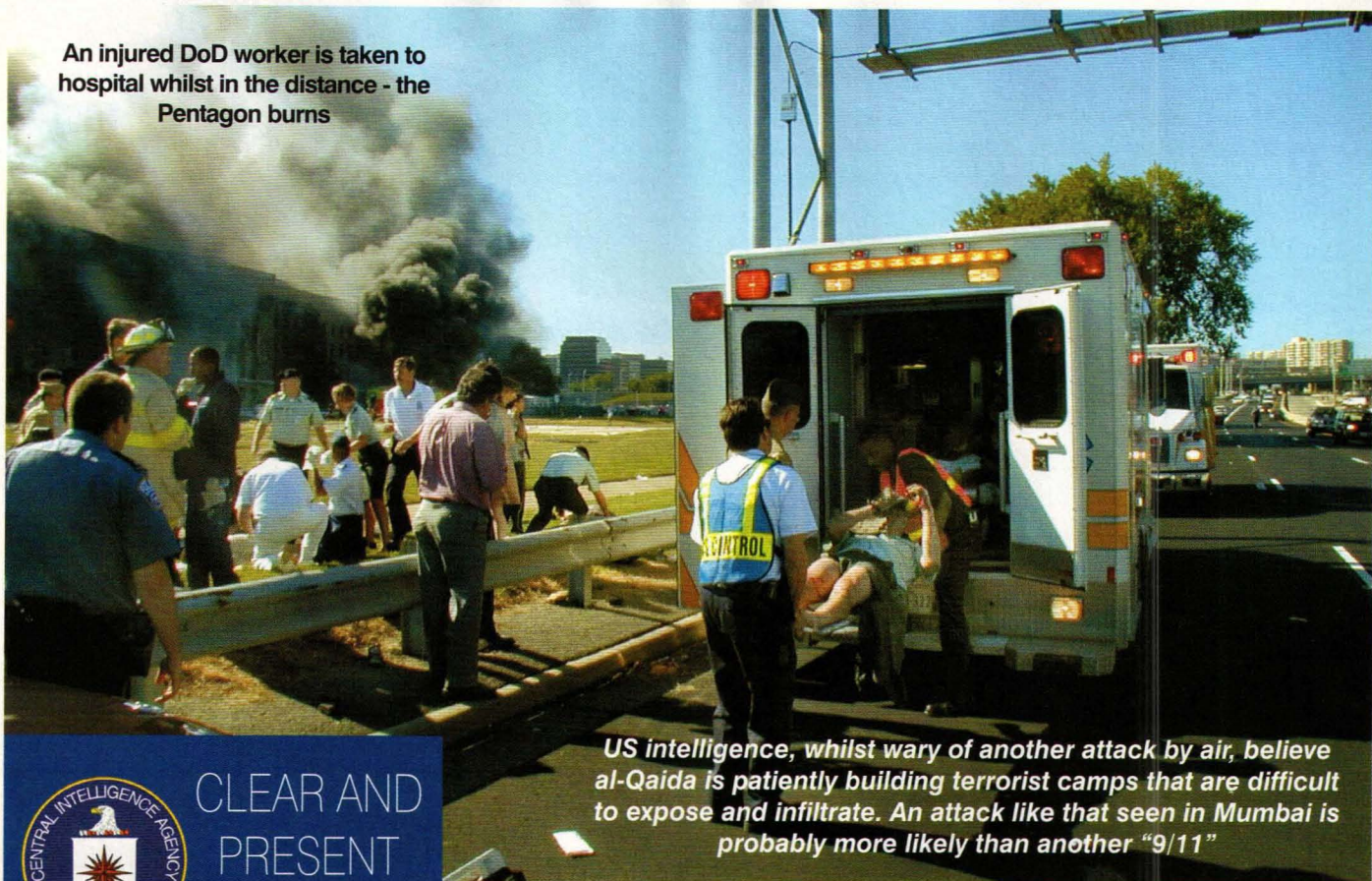


وعدو استجابتك لمطالبنا ومطالب العقل
يعلن أنك وشعبك سوف - ياد الله -

COURTESY INTEL CENTER

TERS TALENT

An injured DoD worker is taken to hospital whilst in the distance - the Pentagon burns



US intelligence, whilst wary of another attack by air, believe al-Qaida is patiently building terrorist camps that are difficult to expose and infiltrate. An attack like that seen in Mumbai is probably more likely than another "9/11"



CLEAR AND
PRESENT
DANGER



In 2008, D/CIA Michael Hayden commented on a specific training camp that might be associated with the "new recruits" intent on launching attacks on US soil.

"What I can tell you about is the situation along the Afghanistan-Pakistan border, which presents a clear and present danger to Afghanistan, to Pakistan and to the West in general - and to the United States in particular," General Hayden said.

"They are bringing operatives into that region for training, operatives that wouldn't attract your attention if they were going through the customs line at Dallas with you when you're coming back from overseas.

"They look Western, [people] who will be able to come into this country without attracting the kind of attention that others might."

these young men will one day come home, and, if so, what they might undertake here."

The FBI has embarked upon a programme that it intends will expose al-Qaida's quiet recruiting of Americans, especially from lesser known groups. Others opposed to US policies

on terrorism are entering the United States and willing to cause carnage. Mr Mueller said many do not need visas to travel. "We need to know where the threat is moving, and we need to get there first," he added.

DRAGNET AND MERGERS

Considered a terrorist group by the United States, al-Shabaab has been identified as one of the organisations keen to recruit Somali-Americans. The security services are still probing threats made against the US by the group's commanders.

Al-Shabaab operates from the Horn of Africa and CIA analysts believe the outfit is close to being absorbed by al-Qaida. Outgoing CIA Director Michael Hayden raised the possibility that it is this liaison that could pose a major and direct threat to the USA.

D/CIA Hayden said: "In East Africa, al-Qaida is engaging Somali extremists to revitalise operations. And while there clearly has not yet been an official merger, the leader of the al-Shabaab terrorist group is closely tied to al-Qaida. And the recent bombings in Somalia may have meant, at least in part, to strengthen the bona fides of this group with al-Qaida's senior leaders.

"A merger between al-Shabaab and al-Qaida could give Somali extremists much-needed funding while al-Qaida could then claim to be re-establishing its operations based in East Africa."

Since 2004, the FBI and other security services have monitored the growing rise of al-Qaida influence in Somalia. In 2005, US citizen Daniel Maldonado, a Muslim convert from Houston, travelled to Africa and joined a terror group near Mogadishu. He was eventually arrested in Kenya and pleaded guilty to federal charges linked to his al-Qaida association. Of course once exposed, the FBI had an opportunity to monitor and research his liaisons. In 2008, agents detained another US citizen in Boston as he made his way to Somalia. Tarek Mehanna had been communicating with Maldonado whilst in Africa, who told him, "I'm here fighting."



Daniel Maldonado

Overseas NSA intercepts have proved a valuable source of intelligence. With such data, the FBI now acknowledges that America is not immune to attacks hosted on its own soil.

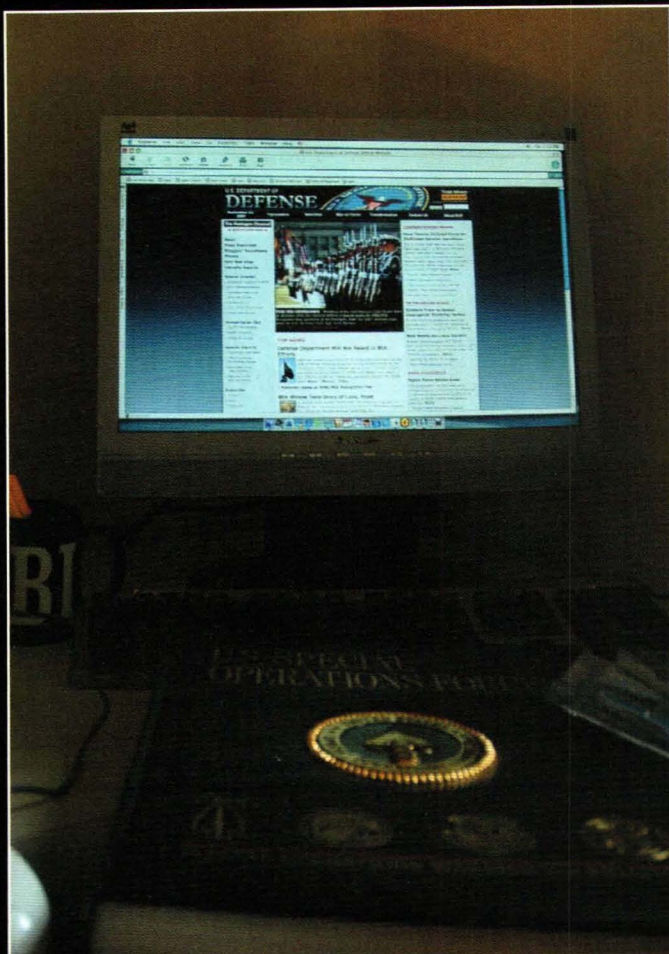
For this reason the US intelligence stress that the "homegrown terrorist" and obscure groups emerging within its own borders are a menace that should not be overlooked. "Some may have little or no actual contact with al-Qaida," said Mr Mueller, "yet fringe organisations can quickly gain broader aspirations and appeal."

British hacker who sent the Pentagon in a spin blames his dangerous action on an obsession with cover-ups and flying saucers



Hacking into any computer is both illegal and dangerous. If you are caught, there is every likelihood you will receive a custodial sentence, unless, of course, you are armed with a warrant. But the stakes get much bigger when the target just happens to be the Pentagon. And not just one computer - nearly one hundred.

Glasgow-born Gary McKinnon may not be a familiar name to most readers of this magazine, but he is probably the most infamous hacker ever to attempt to access the banks of computers that are the lifeblood of the Pentagon. Unlike the crafty cyber buffs employed by Russia, China, Japan and others, McKinnon successfully infiltrated the machines and started a chain of events that have caused ripples on both sides of the 'pond'. The problem for McKinnon, a systems analyst from London, is he got caught, and his balmy hacking exploits just happened to take place shortly after the terrorist attacks on New York City and the



The Hacking Man



A protester outside the US Embassy in London voices his support for Gary McKinnon

© SNAPPERJACK OF LONDON



"I am SOLO. I will continue to



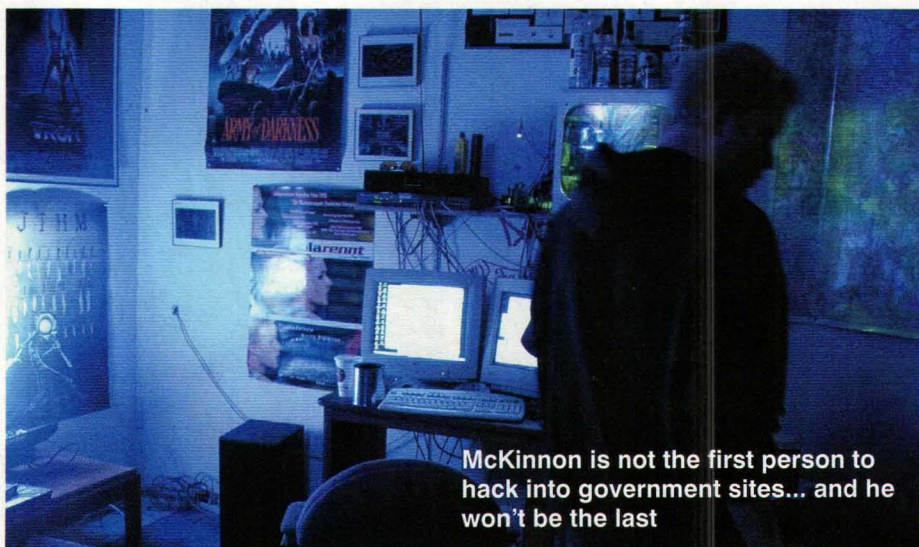
capital in 2001. The timing for McKinnon, now 42, could not have been worse, and the US wants him tried in a Virginia court room.

At the time of the indictment, Paul McNulty, the US Attorney for the Eastern District of Virginia, said: "Mr McKinnon is charged with the biggest military computer hack of all time."

McKinnon admits wending his way into 97 military (army, navy, air force) and NASA computers. But the US legal team also maintain his actions put a further 300 computers out of action at a major naval weapons facility (deleting files). This at a time when the country was facing an uncertain period - the fear of a second terrorist wave. Analysts also believe McKinnon was responsible for bringing down a network of 2,000 US Army computers. A "clean-up" bill of £350,000 for the damage done to the machines has been mentioned by the Pentagon.

At Fort Myer, Virginia, McKinnon is accused of obtaining administrator privileges, transmitted codes, information and commands. He is also said to have deleted over a thousand user accounts. These actions have been described as "malicious", though McKinnon is adamant they were not.

With an extradition paper in hand, McKinnon faces a long period in jail and a \$2m fine if



McKinnon is not the first person to hack into government sites... and he won't be the last

found guilty. Yet most who know McKinnon, actually believe his claim that he was simply searching the Pentagon files for information on aliens... the space kind. And he believes what happened was a "wake-up" call for those who protect the Pentagon computers. In court McKinnon said he was no "web vandal or virus writer," and that he never acted with malicious intent.

So just how easy was it for McKinnon to probe the Pentagon's heart? Using ordinary computers in his London flat, McKinnon discovered that much of the US military use

Windows. By uploading commercial software, McKinnon quickly realised that many machines operated without proper passwords or firewall protection. Since then, the Pentagon and its many arms, have boosted its computer security to such an extent, even the most persistent and professional hackers in the world can't get in. Indeed, the building is "attacked" thousands of times a day by those seeking mischief... and much more.

END GAME

When computer forensic investigators actively began searching for the "hacker", it didn't take long for them to find McKinnon, who by now was starting to leave less than polite messages on screens - including anti-war postings. One message left on a machine at the US Naval Weapons Station Earle in New



The timing of McKinnon's action could not have been worse

Continued on page 24

rupt at the highest levels”

THE PENTAGON

Officials acknowledge the building is constantly under attack from hackers - though security measures and firewalls protecting its computer systems are far better than those in place when McKinnon broke in



US NAVAL WEAPONS STATION EARLE

The Earle Naval Weapons Station, Earle/Leonardo Pier complex, is located along the northern New Jersey shore in the south end of Sandy Hook Bay. It is located 4 miles west of Sandy Hook and 7 miles southeast of Staten Island. The command's name was changed in 1974 from Naval Ammunition Depot to Naval Weapons Station. Earle provides logistical, technical and material support to the fleet in a variety of areas ranging from combat subsystems and retail ammunition management to ordnance packaging, handling and storage.

Since Earle is a weapons station, it handles, stores, transports, renovates and issues all types of weapons and ammunition.

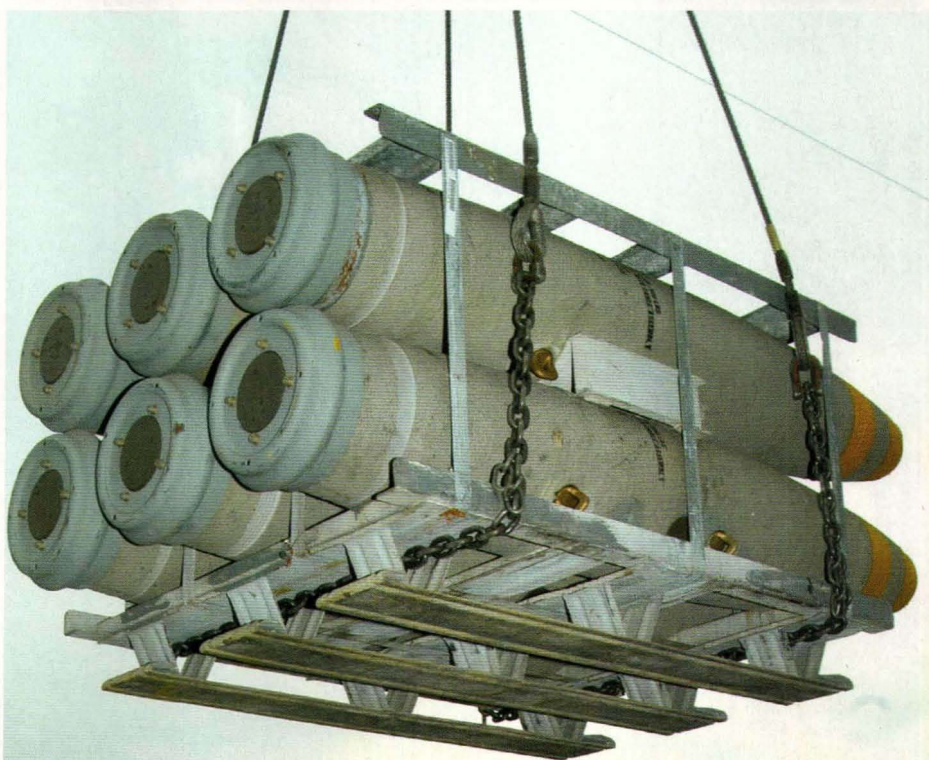
The station - named after RADM Ralph Earle, the Chief of the Bureau of Ordnance during WWI - was commissioned on 13 December 1943 to help with the war effort. When a pressing need developed during World War II for an ammunition depot in the greater New York area, a site in Monmouth County, New Jersey was chosen. The location provided two distinct areas. A waterfront location provided ships with a safe and operationally advantageous port to take on ammunition, while an inland storage area, safe from possible submarine bombardment, provided access to commercial rail facilities with lines coming from the west, where the majority of ammunition shipments originated. On 2 August 1943, construction began and in a short time, storage bunkers, a road and rail network, numerous buildings, and a pier complex were built.

Earle continued to develop after World War II, keeping pace with the changing needs of the Navy.

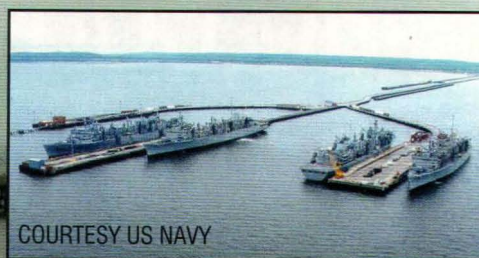
Courtesy: GlobalSecurity.Org

For more information on the Earle facility visit:

LINKS www.GlobalSecurity.org

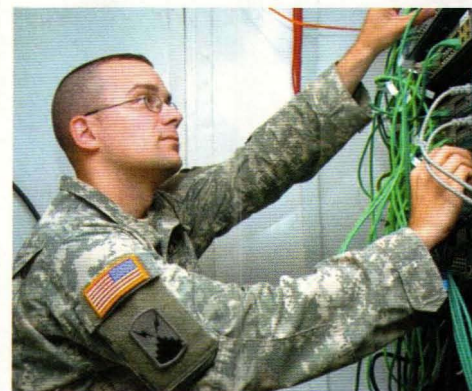


Two Earle personnel oversee another delivery of ordnance



visit
www.eyespymag.com
the world's most
popular independent
intelligence website

100%
SECURE
easy to use
shopping cart!



A US Army engineer carries out maintenance on a major computer system. Some estimates say McKinnon's dabbling with Pentagon computers left the DOD with a bill of nearly \$1m.

Jersey, was particularly "threatening" according to lawyers. It read: *'US foreign policy is akin to government-sponsored terrorism these days? It was not a mistake that there was a huge security stand-down on September 11 last year... I am SOLO. I will continue to disrupt at the highest levels'*.

An electronic trail quickly led to a computer in a house owned by his girlfriend's auntie.

McKinnon rejected a plea bargain which would have resulted in a shorter sentence in return for him pleading guilty. He described his actions as "misguided" but said it felt "like a moral crusade". He earnestly believes the Pentagon is withholding the truth on aliens.

In January, the High Court said it would review the extradition decision - this after it was revealed McKinnon was diagnosed as suffering from Asperger's Syndrome, an autistic condition. During the court hearing, it was revealed McKinnon had at times been suicidal.

Editor's note: McKinnon is terrified about serving time in a US prison, and being treated as a "cyber terrorist". His actions were daft and he probably treated his quest as a game... not too dissimilar to the 1983 movie *'War Games'*. To him it was a super secret adventure, but it was also extremely dangerous and irresponsible coming at a time when 3,000 people had been murdered. I don't think he truly understood he was playing with fire, you simply do not hack a computer... especially those attached to government. Inadvertently, he may have caused ripples that raised the stakes in respect of cyber security, though this is not an excuse or defence.

McKinnon's bizarre quest led to nothing. I suspect he will be sent to America, though I doubt his sentence goes beyond three years. I also suspect he has definitely learned his lesson.

He once said: "What I did was illegal and wrong, and I accept I should be punished. But I am not a member of al-Qaida. I believe my case is being treated so seriously because they're scared of what I've seen. I'm living in a surreal, nutter's film."

That probably sums up this strange episode.

24 Hours a Day
eyespymag.com

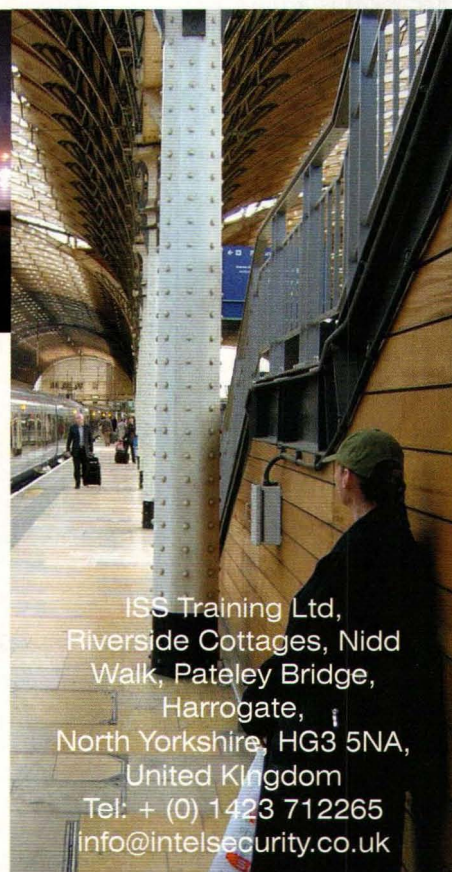
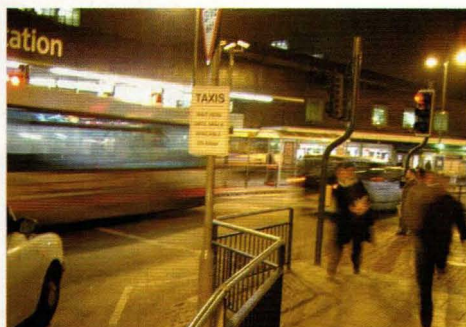
FIVE MILLION HITS A MONTH

ISS

ISS Training Limited are providers of specialist covert surveillance training courses to the security and investigative industry

TOTAL SURVEILLANCE TRAINING

Formed in 1990, ISS is the longest established surveillance training company in the United Kingdom. Their credibility and reputation is internationally acclaimed. ISS offer nationally recognised qualifications.



ISS COURSES:

- Foot & Mobile Surveillance
- Advanced Surveillance
- Electronic Surveillance
- Foot Surveillance Training in London
- Counter Surveillance For Close Protection Officers
- Rural Surveillance
- Tactical Firearms & Surveillance in Switzerland

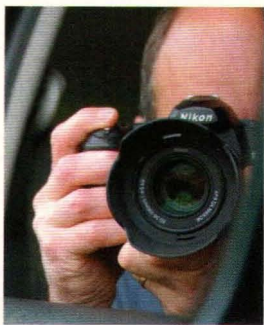


edexcel



ncfe

ISS Training Ltd,
Riverside Cottages, Nidd
Walk, Pateley Bridge,
Harrogate,
North Yorkshire, HG3 5NA,
United Kingdom
Tel: + (0) 1423 712265
info@intelsecurity.co.uk



New anti-terrorism law on photography provokes unrest with civil liberty groups, professional and amateur snappers alike

Civil liberty groups in the UK, and members of the country's leading media union - the National Union of Journalists (NUJ), are up in arms about a new law that makes taking photographs of police officers, just a little more difficult. Section 76 of the Counter Terrorism Act, introduced in February, is designed to give the security services more power when dealing with persons who could be taking images for criminal or terrorist purposes. It's also likely the law was introduced to protect the identity of personnel who by necessity, must remain anonymous.

What concerns NUJ officials and their members, is that junior or inexperienced

police officers, for example, may take exception to photographers who want to try and capture moments that truly reflect an incident or scene. After all, some of the greatest photographs of all time are taken by photographers who often risk their lives trying to freeze-frame incidents or situations. With the threat of a criminal record and up to ten years in jail, the "art" of photography and essentially "visual reporting", could be severely hindered.

Section 76 permits the arrest of absolutely anyone found "eliciting, publishing or communicating information relating to members of the armed forces, intelligence services and police officers, and which is likely to be useful to a person committing or preparing an act of terrorism." That's a fairly broad agenda, and one that is packed with disputable caveats and clearly open to individual interpretation.

For magazines such as Eye Spy, which is visually relevant to the intelligence and

security world, it does pose a problem. The public need to see images of the police at work, in real situations and in control. The imagery taken moments after the London bombings portrayed a real sense of urgency, laced with compassion and professionalism. Not to have published any picture of the police or the security and emergency services would have been just plain daft. We believe it is all about context and can see the intention of the law is to protect, however, the law must be used correctly, and in the spirit it was originally conceived.

If an undercover officer or intelligence officer is photographed (the law applies to the intel services and armed forces as well) even accidentally, and then that image is published, it could of course compromise his or her role. Such a situation occurred moments after the shooting of the innocent Brazilian, Jean Charles de Menezes in London in 2005. CO19 armed officers were caught on camera leaving the Tube station. Yet their faces were pixelated

Section 76 Counter Terrorism Act

TAKING PICTU



by responsible publishing houses who chose to reproduce them. However, they could have found their way overseas and/or onto the Internet. Quite frankly, that may have been a little problematic as someone, somewhere, might have recognised the men.

Because most people carry cell phones with photographic capability, it's becoming more and more likely that images of incidents will occur and be transmitted in seconds. Eye Spy has been told that government officials regard the Internet and cell phone imagery transfer as a growing "problem area".

Continued on page 82



© SNAPPERJACK OF LONDON



An unconcerned 'snapper' at the New Scotland Yard demonstration



© SNAPPERJACK OF LONDON

SIMILAR CONCERNS - STATE-SIDE

NEW YORK CITY: Like London, another city that sometimes lives on its nerves, is New York. And just like London, the threat of terrorism, reconnaissance and intelligence collection by shadowy figures, often leads to police stops. But a recent incident in the city probably reflects how difficult it is to balance civil liberties with security awareness.

Photographer Robert Taylor was taking pictures in the Bronx subway when an officer confronted him. He was told "no photographs", and 9/11 was brought up in the conversation. Taylor said there was no law against such an action, but he was arrested anyway and charged with "disorderly conduct and impeding traffic".

It is our understanding the Metropolitan Transportation Authority did try and ban photography, but it was never passed in law. New York Times reporter, Jim Dwyer, commented on the incident: "Even so, people taking pictures in the subways are regularly stopped by the police and asked to let the officers see their images or to delete them."

Rule 1050.9 (c) of the New York state code says: "Photography, filming or video recording in any facility or conveyance is permitted except that ancillary equipment such as lights, reflectors or tripods may not be used." In London's Tube, photography is not permitted, and if you are seen taking a picture, you are most likely to hear Tube officials announcing over the tannoy "no photography".



ISSUE 9 REF: ES/09 UK £3.50 USA ROW \$7.00	ISSUE 10 REF: ES/10 UK £3.50 USA ROW \$7.00	ISSUE 11 REF: ES/11 UK £3.50 USA ROW \$7.00	ISSUE 12 REF: ES/12 UK £3.50 USA ROW \$7.00	ISSUE 13 REF: ES/13 UK £3.50 USA ROW \$7.00	ISSUE 14 REF: ES/14 UK £3.50 USA ROW \$7.00	ISSUE 15 REF: ES/15 UK £3.50 USA ROW \$7.00	ISSUE 16 REF: ES/16 UK £3.50 USA ROW \$7.00
ISSUE 17 REF: ES/17 UK £3.50 USA ROW \$7.00	ISSUE 18 REF: ES/18 UK £3.50 USA ROW \$7.00	ISSUE 19 REF: ES/19 UK £3.50 USA ROW \$7.00	ISSUE 20 REF: ES/20 UK £3.50 USA ROW \$7.00	ISSUE 21 REF: ES/21 UK £3.50 USA ROW \$7.00	ISSUE 22 REF: ES/22 UK £3.50 USA ROW \$7.00	ISSUE 23 REF: ES/23 UK £3.50 USA ROW \$7.00	ISSUE 24 REF: ES/24 UK £3.50 USA ROW \$7.00
ISSUE 25 REF: ES/25 UK £3.50 USA ROW \$7.00	ISSUE 26 REF: ES/26 UK £3.50 USA ROW \$7.00	ISSUE 27 REF: ES/27 UK £3.50 USA ROW \$7.00	ISSUE 28 REF: ES/28 UK £3.50 USA ROW \$7.00	ISSUE 29 REF: ES/29 UK £3.50 USA ROW \$7.00	ISSUE 30 REF: ES/30 UK £3.50 USA ROW \$7.00	ISSUE 31 REF: ES/31 UK £3.50 USA ROW \$7.00	ISSUE 32 REF: ES/32 UK £3.50 USA ROW \$7.00
ISSUE 33 REF: ES/33 UK £3.50 USA ROW \$7.00	ISSUE 34 REF: ES/34 UK £3.50 USA ROW \$7.00	ISSUE 35 REF: ES/35 UK £3.50 USA ROW \$7.00	ISSUE 36 REF: ES/36 UK £3.50 USA ROW \$7.00	ISSUE 37 REF: ES/37 UK £3.50 USA ROW \$7.00	ISSUE 38 REF: ES/38 UK £3.50 USA ROW \$7.00	ISSUE 39 REF: ES/39 UK £3.50 USA ROW \$7.00	ISSUE 40 REF: ES/40 UK £3.50 USA ROW \$7.00
ISSUE 41 REF: ES/41 UK £3.50 USA ROW \$7.00	ISSUE 42 REF: ES/42 UK £3.50 USA ROW \$7.00	ISSUE 43 REF: ES/43 UK £3.50 USA ROW \$7.00	ISSUE 44 REF: ES/44 UK £3.50 USA ROW \$7.00	ISSUE 45 REF: ES/45 UK £3.50 USA ROW \$7.00	ISSUE 46 REF: ES/46 UK £3.75 USA ROW \$7.00	ISSUE 47 REF: ES/47 UK £3.75 USA ROW \$7.00	ISSUE 48 REF: ES/48 UK £3.75 USA ROW \$7.00
ISSUE 49 REF: ES/49 UK £3.75 USA ROW \$7.00	ISSUE 50 REF: ES/50 UK £3.75 USA ROW \$7.00	ISSUE 51 REF: ES/51 UK £3.75 USA ROW \$7.00	ISSUE 52 REF: ES/52 UK £3.75 USA ROW \$7.00	ISSUE 53 REF: ES/53 UK £3.75 USA ROW \$7.00	ISSUE 54 REF: ES/54 UK £3.75 USA ROW \$7.00	ISSUE 55 REF: ES/55 UK £3.75 USA ROW \$7.00	ISSUE 56 REF: ES/56 UK £3.75 USA ROW \$7.00
ISSUE 57 REF: ES/57 UK £3.75 USA ROW \$7.00	ISSUE 58 REF: ES/58 UK £3.75 USA ROW \$7.00	ISSUE 59 REF: ES/59 UK £3.75 USA ROW \$7.00	ISSUE 60 REF: ES/60 UK £3.75 USA ROW \$7.00	VOLUME 8			

EYE SPY INTE
BACK

VOLUME
2



For full content information on all
Eye Spy back issues visit
www.eyespymag.com

VOLUME
3

VOLUME
4

VOLUME
5

VOLUME
6

VOLUME
7

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

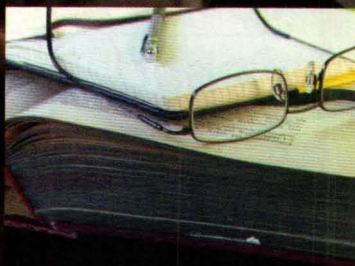
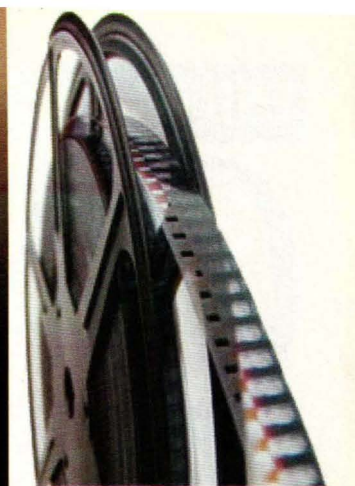
ORDER ON-LINE
www.eyespymag.com

**OR USE ORDER
FORM ON PAGE 82**

ORDER BY PHONE:
UNITED KINGDOM,
EUROPE & REST
OF WORLD
TELEPHONE:
+ (0)1756 770199
(UK)

**NORTH AMERICAN
READERS
TOLL FREE:**
877 309 9243

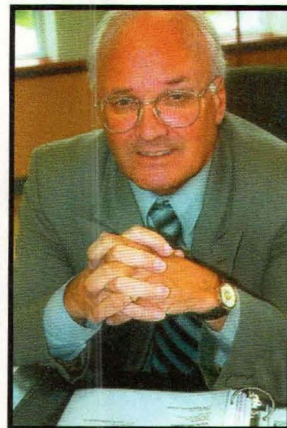
INTELLIGENCE MAGAZINE
ISSUES



END GAME FOR HISTORIC

CAMP 30

Bowmanville



By Eye Spy
Canadian Editor,
Lynn Philip
Hodgson

Now flies across the windswept fields of Camp 30, the buildings now empty. Derelict. In the distance I see the ghostly images of two men walking side-by-side, talking quietly, stately in the tailored uniforms of Hitler's Third Reich. Given their insignia, I see they are Generals. One is General Johann von Ravenstein, second-in-command to Field Marshal Erwin Rommel, captured in the desert of North Africa along with a wealth of information in maps and orders from Adolf Hitler himself. The other is General Artur Schmitt, also captured in Africa while orchestrating this theatre of war, likewise under the command of the 'Desert Fox'.

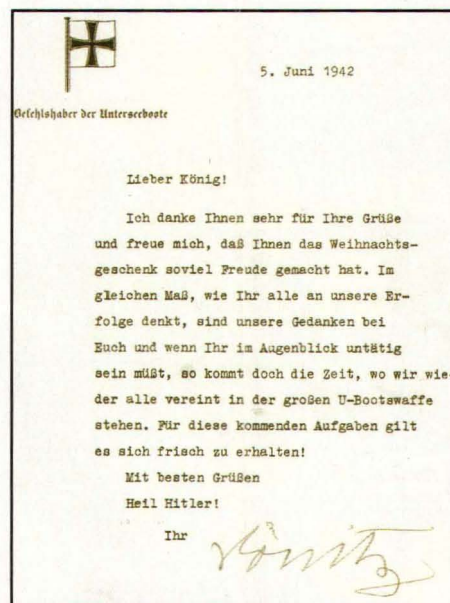
I see the two men are now joined by a third, smartly dressed in his Kriegsmarine uniform, and I quickly identify him as one of the most successful military men of the Third Reich: the Famous Corvettenkapitan, Otto Kretschmer. By the time Kretschmer's U-99 (U-Boat) was

captured in 1941, he had sunk more tonnage than any other U-Boat Commander, including all of those who were never captured. For this, he was awarded the 'Knights Cross with Oak Leaves and Swords' and, while a PoW, was promoted to Fregattenkapitän.

Of course, all of this was just my daydream. I only imagined myself walking in the shadows of such famous people.



Corvettenkapitan, Otto Kretschmer



A letter written by Admiral Donitz to a German PoW at the camp in 1942

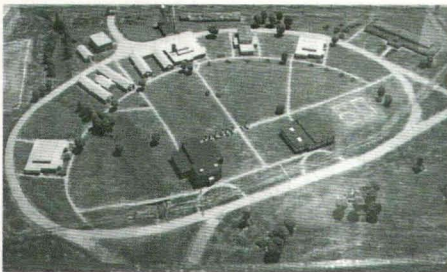
*Canada's historic WWII jewel
faces developer's wrecking ball*



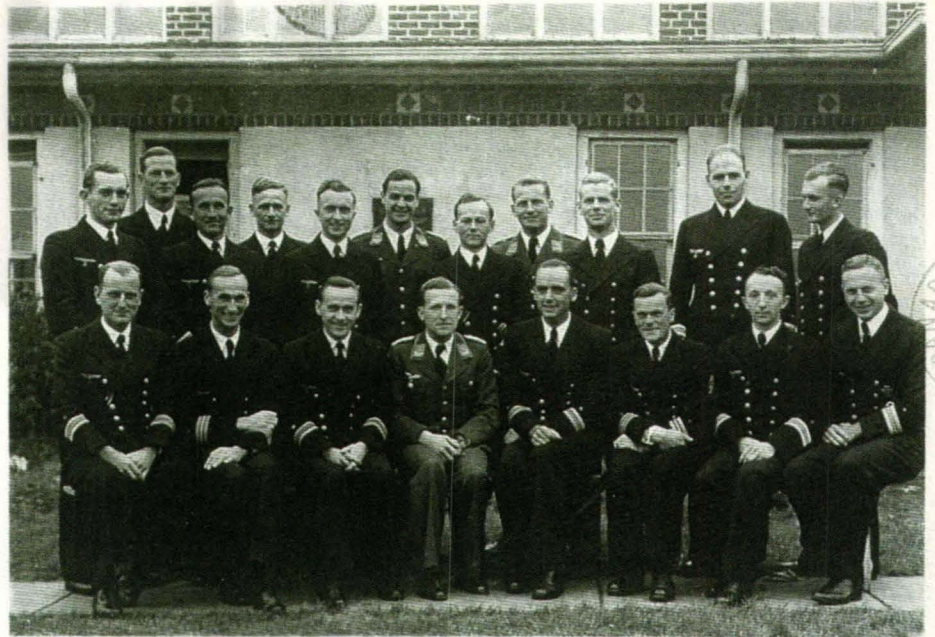
Camp 30 - under construction

Early on in the war, it became evident to the British that they must establish a detention centre for German prisoners of war, especially the officers. The location needed to be secure, still within a Commonwealth country, but as far from Britain as possible. Camp 30 satisfied all these criteria. The British could not afford to take the captured German officers back to Britain: in the event that Germany were to be successful in invading Britain, the German officers would then be released immediately and put back into battle from within Britain. Therefore, the captured German officers were sent to Canada where, ironically, they ended up incarcerated only thirty minutes from the now famous spy camp - Camp-X.

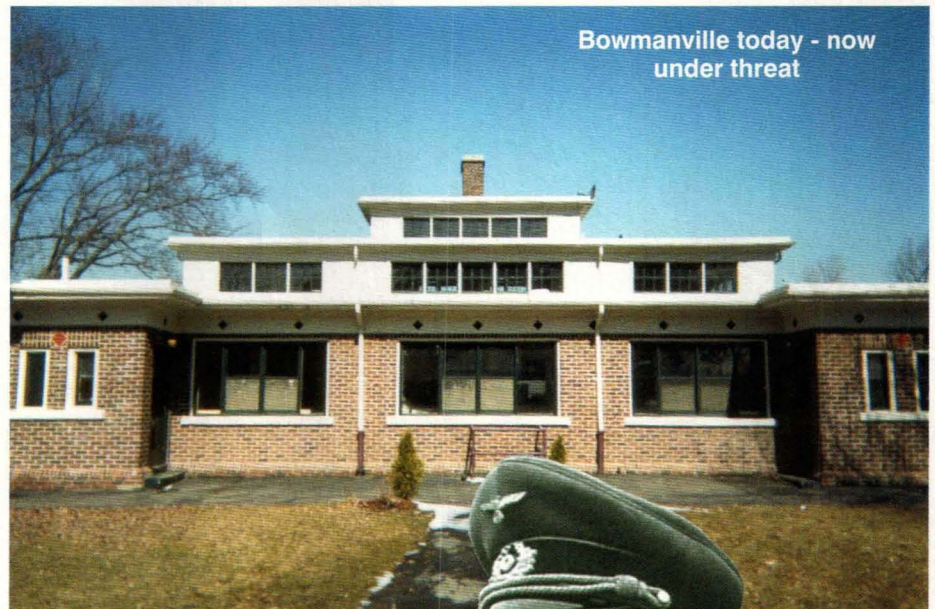
Camp 30 opened on 15 October 1941, and received its first prisoners on 19 November that year. Throughout the War, Camp 30 housed approximately 880 high-ranking German officers. In 1942 the PoWs took over the Camp in what would be famously known as 'The Battle of Bowmanville', but after three hard-fought days, the Germans tired and relinquished their hold on the Camp. ➤



A model of Camp 30 on display at the Bowmanville museum - it is said be the only German PoW camp in the world that is completely intact.

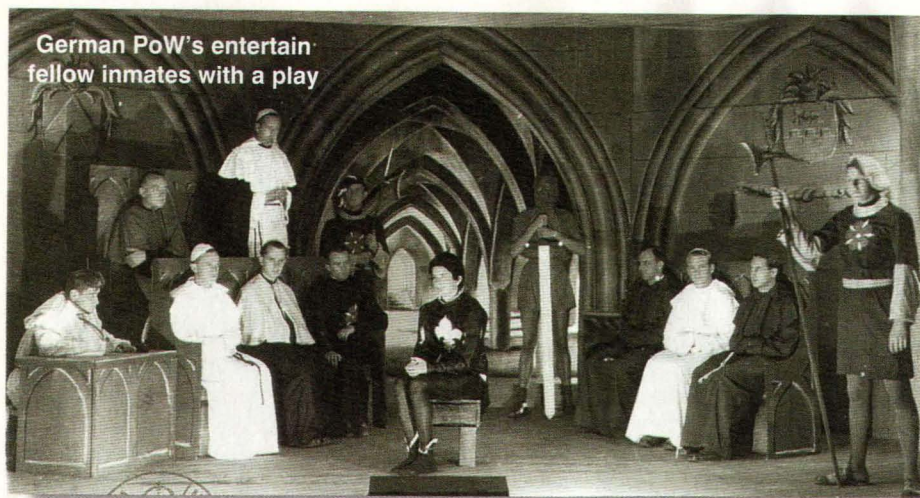


German officers of Camp 30, Bowmanville - Circa 1942



Generalleutnant von Ravenstein and a group photo of PoW's at Camp 30





German PoW's entertain fellow inmates with a play



German PoW Camp 30 orchestra

In early 1943, Admiral Doenitz, Commodore, (Führer der Unterseeboote) ordered the German Command at Camp 30 to arrange for the escape of Otto Kretschmer. Through an elaborately implemented plan, a U-Boat would be waiting for Kretschmer off the coast New Brunswick at Maisonnnette Point on 27 September 1943. The commanding officers had eight months to get him there. An escape plan was begun; a Navy tunnel would be constructed.

Through the summer of 1943, the men worked three shifts daily, tunnelling fifteen feet beneath the building. A sophisticated method for removing the dirt was devised: bag after bag, the earth was placed on a trolley track, then it was lifted from one person to the next until it made its way to the attic of Haus IV. Someone then emptied the bag, sprinkling the earth gently over the rafters. The tunnel extended over three hundred feet, passed under Lambs Road and into a cornfield, a safe distance away from the guards' tower. All went well: the tunnel was completed two weeks before the planned escape. Then all hell broke loose. From here, the story reads like a le Carré novel. But this was fact.

Kretschmer never did make it out of Camp 30 until the end of the war when he was sent to Scotland to attend "de-nazification" Camp 165

Watten, and was finally released in 1947. Kretschmer later wrote a book wherein he stated that had he not been captured and interned at Camp 30 during the war, he would have been murdered by Hitler's henchmen as his name appeared on the list of 5,000 suspected co-conspirators of the failed attempt on Hitler's life on 20 July 1944 at Rastenburg - "The Wolf's Lair".

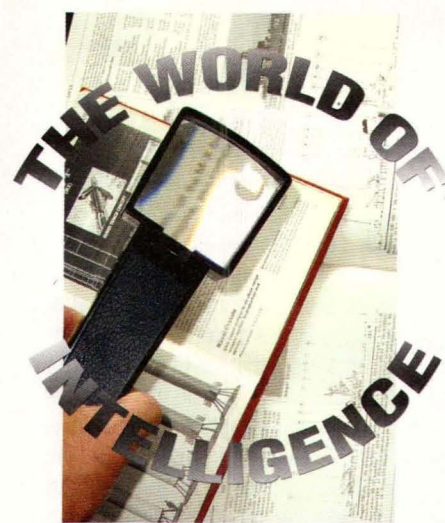
That is all history. Today, this beautiful and historic facility is about to become another victim of "progress" and "development", just like Camp-X and Bletchley Park. Why do we, as Canadians, feel compelled to destroy our past and our identity? Perhaps it is our fear to offend.

If you would like to preserve this very important piece of our history, and to see Camp 30 saved from the wrecking ball, please contact immediately:

The Municipality of Clarington, 40 Temperance Street, Bowmanville, ON, Canada - L1C 3A6 or e-mail:

LINKS: info@clarington.net

For further information regarding the history and significance of Camp 30, please see: www.camp-x.com



THE UK... A POLICE STATE?

"...new legislation playing into hands of terrorists"

The former head of MI5, Dame Stella Rimington, warned that an array of measures intended to bolster security in Britain, is being "exploited by the government" and is "eroding civil liberties."

As new anti-terrorist laws are introduced, including measures to limit photographing police and a massive programme dubbed 'black box', to collect information on e-mail and Web use, Dame Stella says we are playing straight into the hands of terrorists and that Britain risks becoming a "police state."

NO KIM JONG IL DOUBLE

WASHINGTON: New CIA director Leon Panatta, has dismissed suggestions that a double has been used to help keep news of the death of North Korea's leader - Kim Jong il - secret. Panatta, whilst resisting media efforts to divulge his reasoning, admitted he had received confidential information that Kim Jong il suffered a stroke in August 2008, hence he has not been seen in public for months.

Some intelligence watchers believe a 'double' has been used to keep stability in the country. That speculation was fuelled by a book written by Professor Toshimitsu Shigemura who claimed the dictator died in 2003. Shigemura said the double had fooled many world leaders during visits to the country, including Japan's Prime Minister Koizumi.



Kim Jong il and former President Putin... in 2002

RUSSIAN PRESIDENTIAL PRESS AND INFORMATION OFFICE



"Since I have retired I feel more at liberty to be against certain decisions of the Government, especially the attempt to pass laws which interfere with people's privacy," Dame Stella said in an interview with a Spanish newspaper.

"It would be better that the Government recognised that there are risks, rather than frightening people in order to be able to pass laws which restrict civil liberties, precisely one of the objects of terrorism: that we live in fear and under a police state," she said.

Dame Stella, 73, who became the first female MI5 director in 1992, has become a critic of the government's counter-terrorism plans, but when asked about MI5's alleged involvement in the torture of suspected terrorists, she said "while the British secret services were no angels they did not kill people."

COLD WAR GAMES

Canada intercepts Russian bomber



Canadian war planes intercepted a Russian Tu-95 'Bear' long-range strategic bomber just hours before President Barack Obama visited Ottawa. Intelligence watchers believe the timing of the flight and its route via the Arctic, were not coincidental. Two jets attached to NORAD approached the Russian aircraft as it neared Canadian airspace.

Officials who have noticed a major increase in such reconnaissance flights, said the fighter pilots signalled the Russian bomber crew to turn around immediately. This it did about 190 km northeast of Tuktoyaktuk, N.W.T.

Defence Minister Peter MacKay said: "I'm not going to stand here and accuse the Russians of having deliberately done this during the presidential visit, but it was a strong coincidence," he said of the 18 February flight.

A Canadian Air Force CF-18 Hornet, "parallels" Tu-95 Bear in September 2007

An unnamed Russian military official responded: "The Canadian defence minister's statements concerning the flights of our long-haul aircraft are totally unclear. The countries adjacent to the flight path had been notified and the planes did not violate the airspace of other countries. In this light the statements by the Canadian Defence Ministry provoke astonishment and can only be called a farce."

In recent months, Russia's navy has also started to make more journey's to this part of the world. Indeed, a submarine recently dropped Russian flags on the ocean bed claiming the territory as its own. Several countries are locked in a fierce debate about this action, as large reserves of oil and minerals are plentiful in the Arctic.



Defence Minister
Peter MacKay

Tu-95's have also been intercepted by the RAF and Japan recently claimed a Russian bomber had entered Japanese airspace.

AUSTRIAN ASSASSINATION

More eyes on Moscow Underworld

Austria's security services have been accused of not pursuing more aggressively the killers of a prominent Chechen dissident.

Umar Israilov, 27, was shot dead in January as he left a grocery shop near his apartment in Vienna. He had earlier complained to police, that he was being surveilled by probable Russian agents.



Umar Israilov

Israilov, a former insurgent, was also one-time bodyguard to Chechnya's pro-Kremlin president Ramzan Kadyrov. After that, he fled to Austria, and in recent times he has become a high-profile and outspoken critic of the president.

Probably relevant to the case, he was also a witness to the alleged atrocities of a Russian general in Chechnya.

His assassination was described as a "professional hit". Eye witnesses saw two men track Israilov, across the road. To try and lose his followers, Israilov "zig-zagged" through traffic, but he tripped and fell.

"Two men stormed up to him... the man had a pistol in his hand," said one witness. Another added: "We heard shots. The street was full of people. One customer fled into a doorway. The two killers were wearing military trousers." The police have no idea who was behind the assassination but did



release a photofit of one of Israilov's killer (above).

Oleg Orlov, the director of Moscow's Memorial Human Rights Centre, said: "We are deeply alarmed about what appears to be another politically motivated killing of a critic of high-level Russian government officials."

Colonel Bruce Vargo, the joint detention group commander at Guantánamo Bay, gives a tour of a detainee holding cell to Admiral Mike Mullen, Chairman of the Joint Chiefs of Staff

WIRING AND SHARING INTELLIGENCE

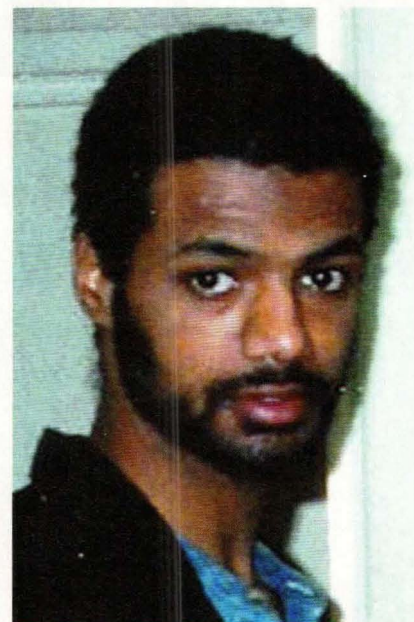
The Case of Binyam Mohamed

According to two senior British High Court judges, US intelligence - threatened to stop liaising with their counterparts in the UK, if secret data concerning a Guantánamo Bay detainee, were released to the public (re: a State Department letter dated 21 August 2008). The supposed threat surrounds Ethiopian-born Binyam Mohamed, who claimed asylum in Britain when he was 16. Mohamed was detained in 2002 in Pakistan after he tried to board a flight to the UK on a false passport. US intelligence had collated information on Mohamed, who allegedly trained in Afghanistan in the summer of 2001, at an al-Qaida terrorist camp.

It was in Afghanistan that the CIA allege Mohamed liaised with former Chicago 'gang member' Jose Padilla. Padilla and Mohamed are said to have been ordered by Osama bin-Laden to attack

targets in the US using a dirty radiological bomb and cyanide. Padilla was detained at Chicago's O'Hare Airport on his return from Afghanistan, and though the primary terrorist charges against him were lessened to "conspiracy and material support for terrorism", he was still sent to prison. Mohamed, meanwhile, according to his solicitors, had travelled to Afghanistan to "resolve personal issues".

Before Mohamed ended up at Guantánamo Bay in 2004, the US say he admitted various terrorist offences. However, Mohamed's legal team say much of what was imparted was done using torture, and without the shield of a lawyer. Similarly, Mohamed says he was the victim of extraordinary rendition - which saw him being transferred to several covert centres for interrogation. It has also been said that while he was captive, MI5 officers interviewed Mohamed and provided questions to their US colleagues to ask



and Obama's Guantánamo Conundrum

CE

For a number of years - Chicago gang member Jose Padilla was linked to a terror plot that involved detonating a radiological bomb. The charges were ultimately dropped - but Padilla was jailed for "association"



him. Some critics say this amounts to collusion in the torture allegations.

In 2008, the UK asked America that Mohamed be returned along with four other persons. This in turn raised the prospect of US intelligence being discussed in a British court. Mohamed's solicitor wanted the UK government to publish a US-compiled dossier about their client's treatment in Afghanistan, Pakistan and Morocco. There then followed a series of letters between John B Bellinger (US State Department) and Lord Justice Thomas

and Mr Justice Lloyd Jones (21 - 28 August 2008) which discussed the possibility of materials about the Mohamed affair being made public.

In February, the two judges publicly criticised Washington by revealing what was actually written.

The UK Government was told: "We want to affirm in the clearest terms real that the public disclosure of these documents or the information contained therein is likely to result in serious damage to US national security and could harm existing intelligence information-sharing arrangement between our two governments.

US security troops pictured in 2002 at Camp X-Ray (now defunct) await the arrival of prisoners



Despite this, both Lord Justice Thomas and Mr Justice Lloyd Jones said it was in the "national interest" to comply. "It would not be in the public interest to expose the UK to what the Foreign Secretary still considers to be the real risk of the loss of intelligence so vital to the safety or our day-to-day life."

Legal boffins and some observers (including journalists) took this as meaning the CIA and other US intelligence entities were basically pressurising the government with threats of non-cooperation with the likes of MI6 and MI5.

There is no doubt to the seriousness of the letter, and John Bellinger may have chosen his words a little more carefully, especially ➤



The case of Mohamed and the supposed crack in UK-US intelligence relations, came just hours after David Miliband met with Hillary Clinton, United States Secretary of State in Washington, DC.

Soldiers monitor part of the prison known as Camp X-Ray (now defunct)

August 21, 2008

Daniel Bethlehem, QC
Foreign & Commonwealth Office
King Charles Street
London, SW1A 2AH

Dear Mr. Bethlehem,

I write with respect to proceedings in your courts regarding Mr. Binyam Mohamed.

We note the classified documents identified in your letters of June 16 and August 1, 2008 to the Acting General Counsel of the Department of Defense. We want to affirm in the clearest terms that the public disclosure of these documents or of the information contained therein is likely to result in serious damage to U.S. national security and could harm existing intelligence information-sharing arrangements between our two governments.



US to communicate such material in confidence to the UK is protected. Without such confidence they will simply not share that material with us."

All charges were dropped against Binyam Mohamed in October 2008. He returned to Britain on 23 February accompanied by specialists from New Scotland Yard, the Foreign Office and his legal team.

Mohamed's legal team issued a statement on his behalf: "I have to say, more in sadness than in anger, that many have been complicit in my own horrors over the past seven years.

"For myself, the very worst moment came when I realised in Morocco that the people who were torturing me were receiving questions and materials from British intelligence."

considering the illuminated liaison and cooperation that has existed between the intelligence services of both nations for decades. However, some intel watchers believe it was the UK which asked for the comment to be inserted - effectively placing all the blame on the USA. Of course had critics considered the wider picture and understood how intelligence agencies across the globe operate and liaise, they would have recognised it was definitely not a threat. Intelligence constantly flows from one country to another and visa-versa where cooperation exists. In all cases it does so on the *proviso* it does not get released to the public unless its primary source agrees. Three years ago the UK's security services were privately fuming when British intelligence photographs of a number of improvised explosive devices - recovered

following the failed 21/7 bombings - found their way into the US media. These images had been wired to a federal service on the eastern seaboard.

Britain's Foreign Secretary David Miliband, was quick to deflate the comments of many mischief makers who had misconstrued the comments, and how intelligence sharing worked. "The issue at stake is not the content of the intelligence material but the principle at the heart of all intelligence relationships - that a country retains control of its intelligence information and it cannot be disclosed by foreign authorities without its consent," he said. "That is a principle we neglect at our peril." He went on: "Our intelligence relationship with the US is vital to the national security of the UK. It is essential that the ability of the

NO MI5 RECOLLECTION

Part of the controversy surrounding Mohamed concerns the exact date when he actually confessed - before the alleged torture, or after it. His legal team believe much light could be thrown on this if the US dossier and over 40 pages of other material is fully released and digested, and if MI5 acknowledge certain allegations put to them.

In July 2008, at the High Court, an MI5 intelligence officer known as 'Witness B', was called to provide details of his meeting with Mohamed in jail in Pakistan. It was a rare event.

The MI5 officer was asked if he had questioned Mohamed about the possibility he had been tortured or mistreated in detention. "I do not recall whether I asked him in exactly those terms," replied Witness B.

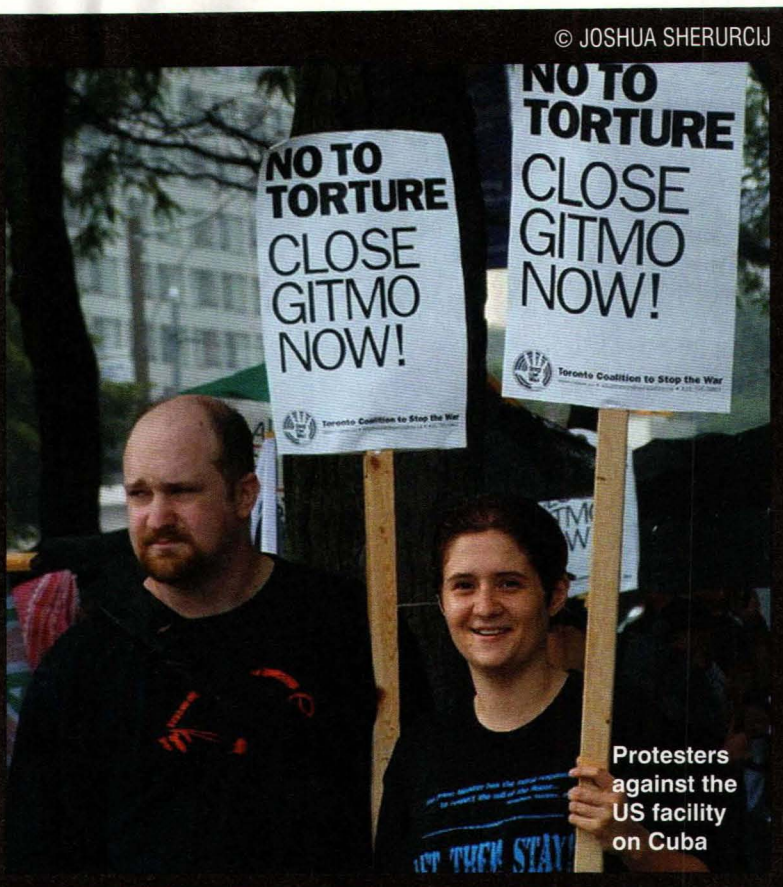
Further questions were put to the MI5 officer by Dinah Rose QC.

DRQC: Not in exactly those terms. But in the substance of that question?

Witness B: I do not recall whether I asked him in the substance of that question.

DRQC: The truth is that you did not, did you?

Witness B: As I said, I do not recall whether I did or not.



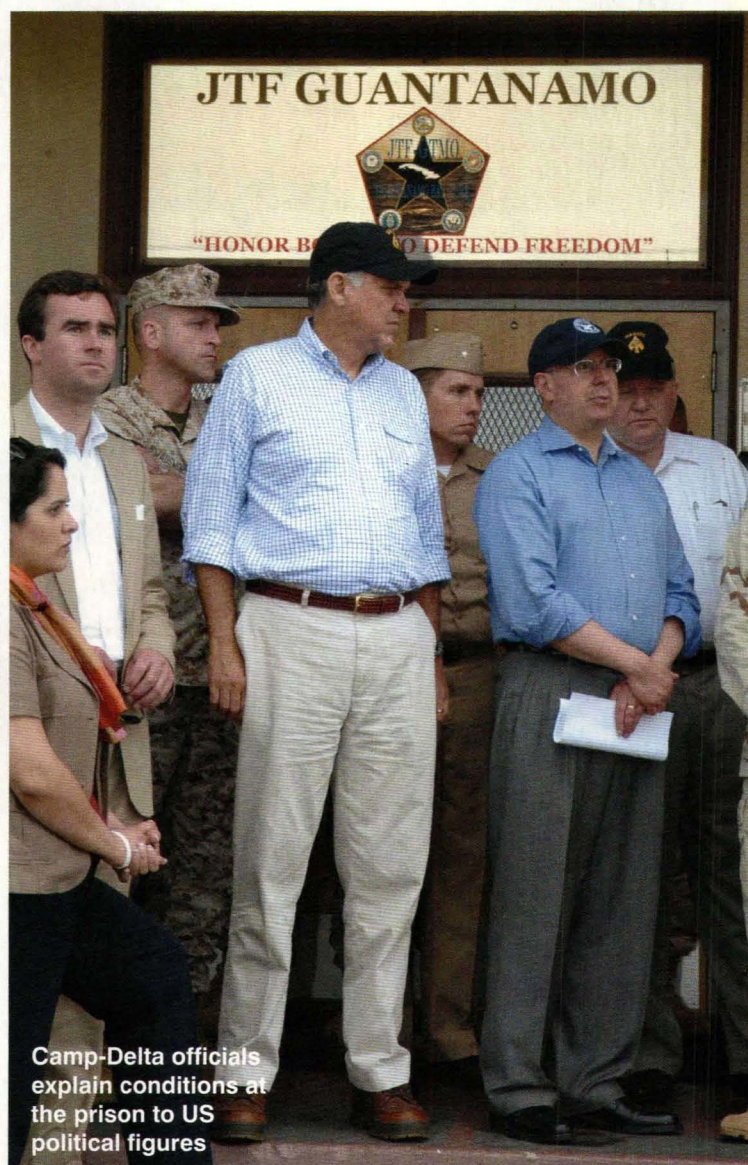
Protesters against the US facility on Cuba

SECURITY HEADACHE

Some released inmates have resumed their fight against America and the West...



It was one of President Obama's first directives - to announce the closure of Guantánamo Bay, the top security military (JTF - Joint Task Force) controlled prison on the island of Cuba. It's a decision Obama had already made during months of campaigning for office, and he was keen to rush through this promise. Besides being a vote winner, it was welcomed by leaders of the international community and by elements in the US military, but not all. However, signing off the end of the controversial facility has generated its own problems, not least the fate of the 245 or so detainees - many of whom are known terrorists, others suspected of terrorist actions. ➤



Camp-Delta officials explain conditions at the prison to US political figures

European countries have long called for the closure of the prison, and even though Obama has requested that countries such as Great Britain, Germany, France and Spain, take back their own nationals (and others), not one European Union nation has agreed.

Allied to the closing of the prison is Obama's other key decision that the CIA shut down or disable, at least for the foreseeable future, a number of "ghost stations" situated around the world. These "pass-through holding and interrogation centres" have caused the CIA to enable huge cover stories in an attempt to conceal the whereabouts of such sites, though one or two stories about their existence have emerged. Most notably, the facility sited within the confines of a Polish military complex.

The emergence of Guantánamo Bay, the extraordinary rendition flights of suspected terrorists and the "ghost stations", are of course, the result of the CIA's huge global terrorist dragnet and from the capture of al-Qaida operatives in overseas military campaigns. With reports of torture and the possible illegal holding of inmates without trial, Obama has seen fit to draw a line under this part of the anti-terrorist operation.

Critics of the move have long argued that many of the operatives held at the Cuban site, if released, will simply "melt" back into the shadowy support outfits and more managed elements that make up al-Qaida.

Obama's predicament has been made even more difficult because, it appears, this warning has come true. Back in 2007, prisoners '372' and '333' were released back to Saudi Arabia for "rehabilitation". But a video released on an al-Qaida support web site shows Said Ali al-Shihri [372] announcing he has been elevated as leader of 'al-Qaida in the Arabian Peninsula in Yemen'. On the same video, Abu al-Hareth Muhammad al-Oufi [333] also speaks about his role as a senior commander in the country. Al-Shihri says his

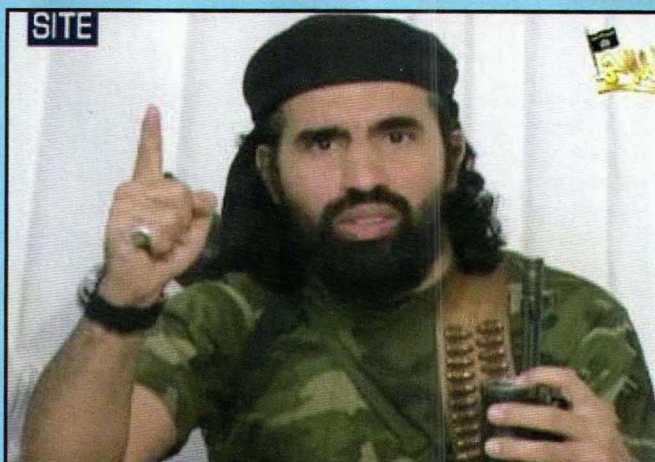
time in prison only made his resolve stronger in jihad (holy war). The Yemeni group has been behind several attacks on the US Embassy in Sana, Yemen's capital.

The CIA estimate 20 former detainees of the 500 or so persons who have passed through Guantánamo Bay have rejoined terrorist groups, and a further 43 have been involved in a variety of terrorist activities, including operations and direct support.

President Obama is said to be trying to find new detention facilities to house the "hard core" elements at Guantánamo, and at the same time, has asked the intelligence services to determine which inmates are harmless enough to be returned to society. That's not going to be easy, as proven by the actions of al-Shihri and al-Oufi - two prisoners assessed and reportedly considered "low risk", despite al-Shihri's background. Two weeks after 9/11, al-Shihri, a terrorist courier, made his way to Afghanistan with a large sum of money used to support fighters. He then trained at an urban warfare camp north of Kabul. Furthering his

career, he liaised with Iranian-based al-Qaida fighters and briefed them on how to enter and bypass security forces on the Afghanistan border. He was captured in December 2001, and became one of the centre's first inmates.

Mr Obama may well live up to his promise to close the prison in January 2010, but the problem - what to do with some inmates - will undoubtedly remain long into his tenure.



Former Guantanamo inmates Said Ali al-Shihri (above) and Abu al-Hareth Muhammad al-Oufi have recently appeared on an al-Qaida video



A Gulfstream 400. The CIA has been accused of using aircraft such as this to shuttle suspected terrorists around the world for interrogation - a procedure called 'extraordinary rendition'

TRADECRAFT

EVOLVING RULES



INTERVIEW AND ANALYSIS

Profiling • Counter Terrorism • Covert Counter-Surveillance

In the aftermath of the 7/7 bombings in London, Adrian Radford a former British Secret Intelligence Services instructor and former member of the acclaimed British Military Intelligence Anti Terrorist Survey Team and author of the Internationally best selling anti surveillance DVD series 'Am I being Watched', takes a look at Counter Terrorism and answers some important questions; Can we actually profile terrorists? What should we now be looking for? and what can profiling do to prevent terrorist attacks at public events and spaces?

Eye Spy: Many agencies and organisations worldwide profile for terrorists. Is this actually feasible?

AR: It is certainly worthwhile. In recent history the profiling of persons at events and public spaces has certainly lead to the positive identification of terrorist subjects. Is it as certain as we would like? I am sorry to say not quite.

Eye Spy: Why is there a doubt in current profiling practices?

AR: Not every terrorist conforms to the exact profile experts have decided upon. Whilst there is a plethora of historic evidence to support current established profiles, conditions are changing, and so must we. Historically the vast majority of terrorists and suicide bombers have been men, however there have been a very small number of female terrorists. It must be expected that open source reporting of incidents has already brought this to the attention of terrorist planners. In response to our current successful profiling of such attackers, more female terrorists are becoming suicide bombers. This is evidenced by increasing attacks by women in Afghanistan and Iraq, where the Taliban and al-Qaida are strongest.

Eye Spy: If the profiling of a terrorist is evolving, what else is changing?

AR: Current profiling has been fixated on younger terrorists, yet only around 40% are aged between 16 and 28. The majority of terrorists are therefore older than 28 years of age. Leaders, recruiters and planners certainly fall within this age group, and it is statistically true that the majority of suicide bombers have been aged between 18 - 25 years. However a fundamental change in response to awareness of this tactic could soon evolve, in order for the al-Qaida terrorists (and its franchises) to stay one step ahead. Therefore current profilers could easily over look an older or female suspect. It is also true that terrorists are now more ethnically diverse than ever before. No one should be discounted, everyone should be suspected.



ADRIAN RADFORD explains how profiling can be augmented by covert counter-surveillance and identifying the traits used by most terrorists

Eye Spy: How can successful profiling tell the difference between an innocent subject, a terrorist conducting reconnaissance and a terrorist about to detonate an explosive device?

AR: It may seem daunting at first to think one can actually differentiate between them, but there are very specific tell-tale signs and its very worthwhile looking into some of these in much greater detail. Most of these guidelines are already common knowledge to the government and security sector, and indeed they have their own systems in place to profile for these. However, there are now a growing number of commercial and civilian organisations, sporting venues and other establishments that are potential targets for terrorist attacks. A number now conduct their own counter-terrorist operations, these would certainly benefit immensely from such knowledge.

Eye Spy: Reconnaissance of targets by terrorists is becoming more prevalent and sophisticated. However, preparation by the security

services, awareness and intelligence collection can prevent attacks. What are some of the actions that should raise red flags?

AR: Before any attack, terror organisations such as al-Qaida will conduct some form of pre-attack reconnaissance and even surveillance. In the preliminary stages of the Terrorist Planning Cycle, initial target selection will be decided upon after any such reconnaissance. Any terrorist involved in this phase of the reconnaissance will generally be relaxed and calm, and will not want to give away their intention or presence. They will therefore make every attempt to blend in with their targets surroundings. They will certainly attempt to conceal their faces to avoid detection and identification from CCTV by wearing baseball caps, hats, scarves or other head gear. It is well established that the use of covert counter-surveillance or surveillance detection drills will identify multiple sightings of repeat terrorist visits. Therefore the only way to successfully identify any form of reconnaissance is the implementation of a knowledgeable and professionally covert counter-surveillance or surveillance detection team. The ability of CCTV operatives in public and private environments should not be overlooked as an effective aid to detect early pre-attack reconnaissance. Any suspect[s] should be approached as early as possible, simply waiting until they might appear next time, thus confirming your suspicions, could lead to a catastrophic event. Sadly this is a very common practice, lethargy breeds unprofessionalism and can

seriously impede the effectiveness of security planning. If in doubt check it out.

The initial phases of target selection and reconnaissance are normally conducted by older, more experienced terrorists, hence the need for change within the profiling environment. Earlier detection can be achieved if a multi-layered defence and an in-depth strategy is adopted,

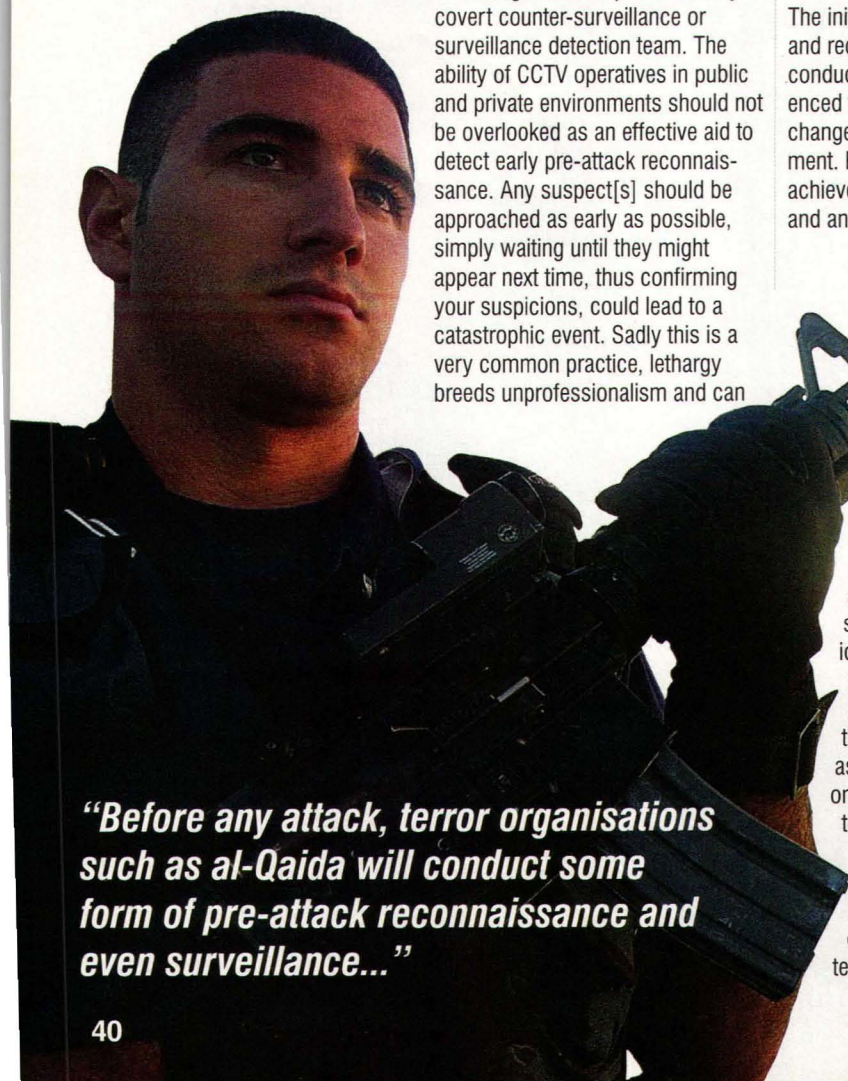
by extending the reach of the security sphere to include covert counter-surveillance. Only skilled surveillance operators trained in a counter-surveillance role have the ability to covertly follow any suspect and successfully identify the specific actions, movements, patterns and behavioural "tell-tale" signs that will identify their suspects as a terrorist, criminal etc. It only takes limited surveillance to identify what exactly the subject is focusing on. At public events and in public spaces pedestrians flow in certain directions, often terrorists involved in the

planning of attacks, by simple nature of reconnaissance itself, will at some stage move against the flow of people traffic. When observed from a static position of elevation is plainly obvious; hence the need for static counter-surveillance to be positioned up high, as is often the case.

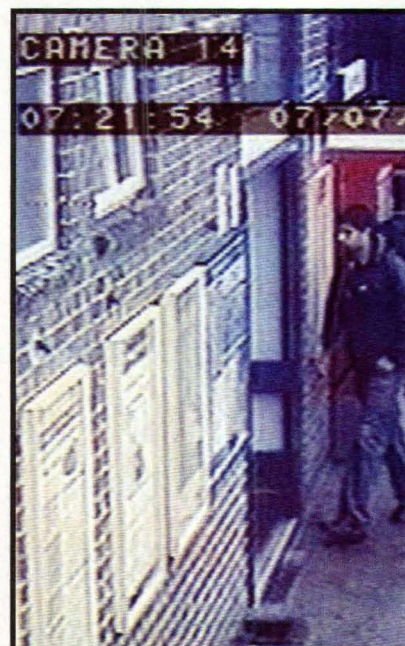
In the later stages of attack, reconnaissance, when the target has been chosen, it is normal for the actual attackers that will

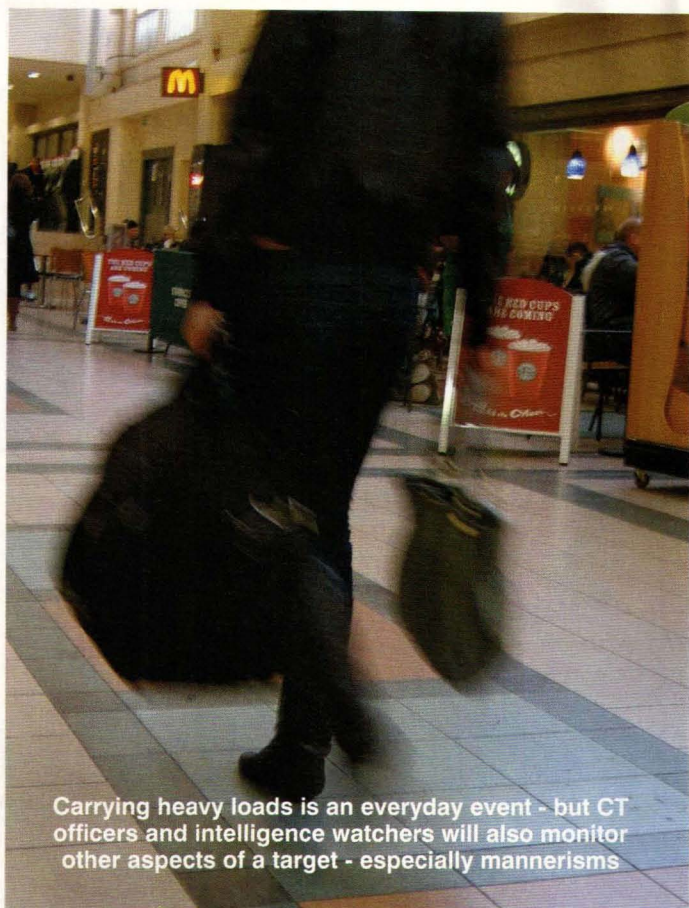


CHECKPOINT: Security officers manning such posts are given careful guidance and training - especially in vulnerable areas prone to suicide bombers and terrorist attacks



"Before any attack, terror organisations such as al-Qaida will conduct some form of pre-attack reconnaissance and even surveillance..."





Carrying heavy loads is an everyday event - but CT officers and intelligence watchers will also monitor other aspects of a target - especially mannerisms

eventually carry out the attack to conduct their own pre-attack reconnaissance in the later stages of the Terrorist Planning Cycle. This will be conducted in a calm but assertive and dedicated manner, they will be more intrusive than initial reconnaissance and will again certainly attempt to conceal their faces and fade into their targets surroundings. Again, this is where skilled covert counter-surveillance or surveillance detection will again identify repeat sightings of potential

terrorists. If an establishment has been the subject of preliminary target reconnaissance, the presence of further, probably younger potential terrorist suspects confirms the targets selection for attack, and thus early identification can recommend the proportionate increased security measures required, commensurate with the threat and the perceived value of an attacks success against the establishment or event.

Eye Spy: How do those conducting the initial reconnaissance differ to the behaviour exuded by actual suicide bombers?

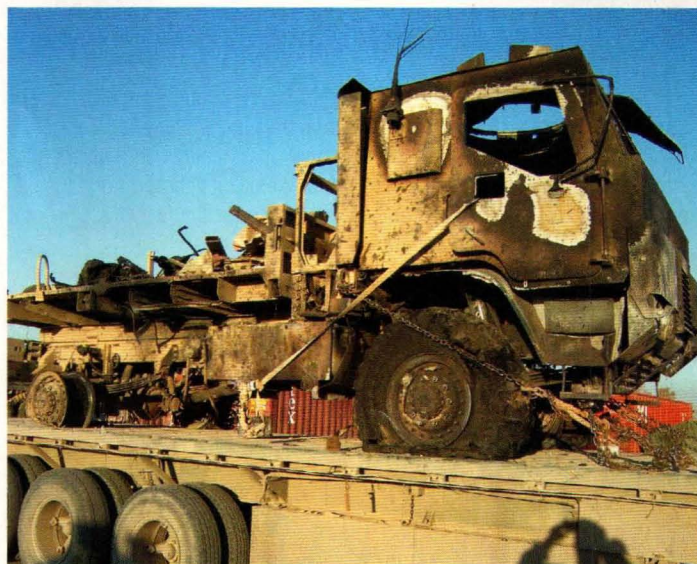


Relaxed, focused and uniform ready. The 7/7 London bombers embark on their journey to the capital. Their targets had already been reconnoitred weeks earlier

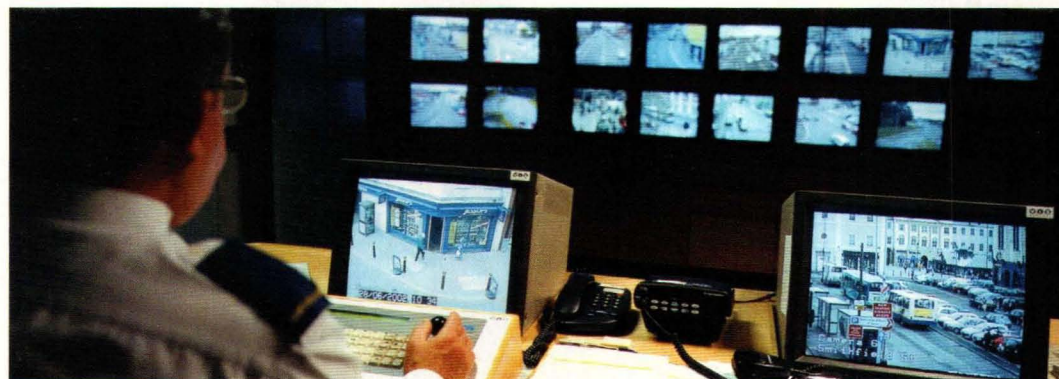
TECHNOLOGY AND OBSERVATION



A business development manager for US contract company Vectronix Inc., uses infrared technology to look for simulated improvised explosive devices being carried by test subjects at Hanscom Air Force Base. The tests being conducted by the Air Force Counter IED Office at Hanscom are expected to pinpoint technologies that can reduce suicide bombing threats in operational theatres.



A suicide bomber strikes in Iraq - leaving seven people dead and 20 injured. Protected by the vehicle's tough exterior, none of the US occupants were killed.



AR: Unlike terrorists conducting pre-attack or preliminary reconnaissance, an actual suicide bomber on an attack run from which they are prepared not to return from alive,

according to evidence available, will display a very different persona indeed, which when profiled and assessed correctly should lead to

the early identification of an imminent suicide bomber. To answer your original and further questions, this is where the difference between normal members of the public and actual suicide bombers can be established. It is important to understand that whilst these guidelines for detection of suicide bombers have been accurate, recent history shows again a change in the idealistic profile and signature behaviour of suicide bombers.

Suicide bombers will in most cases exude an extreme episode of emotion, translated into body language and behavioural changes distinctly from that of their surroundings. Extreme nervousness is certainly a strong characteristic in the minutes before any attack. The presence of significant signs of undue stress plays a major part in defining an imminent attacker. Such terrorists, according to current profile evaluations, will show obvious and apparent signs of nervous stress, touching their faces, neck, repeatedly checking their explosive device being carried under their clothes, or holding onto a bag or rucksack with a vice like grip. Excessive sweating and tunnel-vision have long been associated with the imminent detonation of a body-worn improvised explosive device (IED). In certain circumstances suicide bombers have been observed repeatedly muttering probable religious verse, although this of course cannot ever be fully corroborated.

However, in light of analysis of the 7/11 and 7/7 bombers, these terrorists, even though faced with the imminent certainty of death, did not appear to be in any state of nervousness, instead they were all caught on CCTV and images broadcast throughout the world. They appeared calm, even smiling and laughing with each other before going their separate ways on their final attack runs. Although deeply fanatical and extremist in their beliefs, they successfully suppressed tell-tale emotions. This behaviour suggests that current profiling, however worthwhile and vital, may be vitally flawed if the profilers themselves become tunnel-visioned. Again, we are seeing a potential fundamental change in terrorist modus operandi versus what we have historically profiled. Terrorists are evolving and learning from their successes and failures. So too must the security services.

Eye Spy: If the profiling of suicide bombers is therefore becoming more challenging, can profilers not look to the identification of bags or clothing used in the final stages of attacks?

AR: The early identification of any bag or suspect clothing, wires or bulges will certainly aid a profiler. There is no evidence to support any change in the characteristics of device carriage. Explosives are still worn under garments, often giving the bombers a rigid and noticeable frame, often exposed by bulges in unnatural areas. In an evolving time, profilers should look to assess any

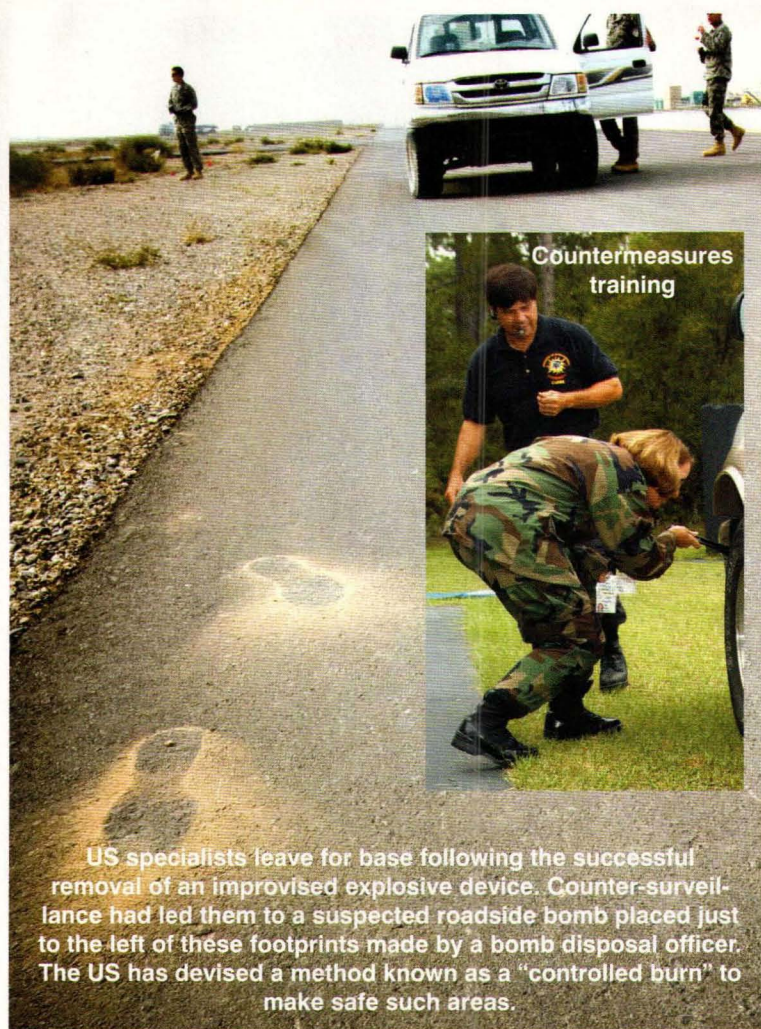
extremely loose or baggy clothing against the fullness of face. Suicide bombers are likely to have been trained at terrorist camps. Instruction will prevent them from "putting on the pounds" that would require such oversized clothing. But it can be observed.

Groups of attackers have commonly concealed their devices in the same type of rucksack or bag - the 7/7

bombers, for example. Identifying like-for-like amongst individual suspects should alert any profiler to an early intervention. Heavy and overstuffed bags remain highly suspect in the profile of a suicide bomber. With recent open source reporting this means of identification should never be considered as an absolute. Yet again, our terrorist profile is evolving. It is important to remember, explosives can be concealed anywhere and in any quantity.

What has not changed is the avoidance of security personnel by suspects during any attack phase. CCTV operatives are more likely to be able to observe a clear path of avoidance than any on-the-ground profilers, however, covert counter-surveillance operators may also be able to close with any suspects and accurately identify any potential terrorist clearly avoiding security guards, or indeed reacting unnaturally to approaches made by overt security personnel.

No longer can profilers depend on identifying signature clothing. Recent terrorist attacks have been conducted by terrorists who have



US specialists leave for base following the successful removal of an improvised explosive device. Counter-surveillance had led them to a suspected roadside bomb placed just to the left of these footprints made by a bomb disposal officer. The US has devised a method known as a "controlled burn" to make safe such areas.



Nerves, sweating and fidgeting exposed shoe bomber Richard Reid as he tried to blow up an airliner enroute to Miami in December 2001



Counter-terrorism training in a semi-urban environment (650th Military Intelligence Group)

lived and worked amongst their targets for many months, even if they have been infiltrated illegally from abroad. They will look, act and dress the same, and will often be educated to a high standard. It takes a certain amount of intellect to successfully plan, recce and carry out a spectacular attack of the kind we have witnessed in recent years. Therefore profilers should actually expect any potential terrorist to dress as any other member of the public might. They will predominantly wear very similar styles of clothing, creating a civilian uniform. This can be an aid for any profiler to detect a number of suspects belonging to the same cell, and they

will predominantly be all of a similar age, as these individuals would have socialised extensively together along with their families. The 7/7 and 21/7 bombers are a good example. Similarities should therefore be prevalent and obvious to the trained eye of a surveillance and counter-terrorist expert.

Eye Spy: Profiled accurately, can suicide bombers be prevented in the final stages of an attack or is too late once they are on their final run?

AR: In the imminent stages of a final approach, profilers can expect suspects to hold their initiation devices tightly. Clear observation of

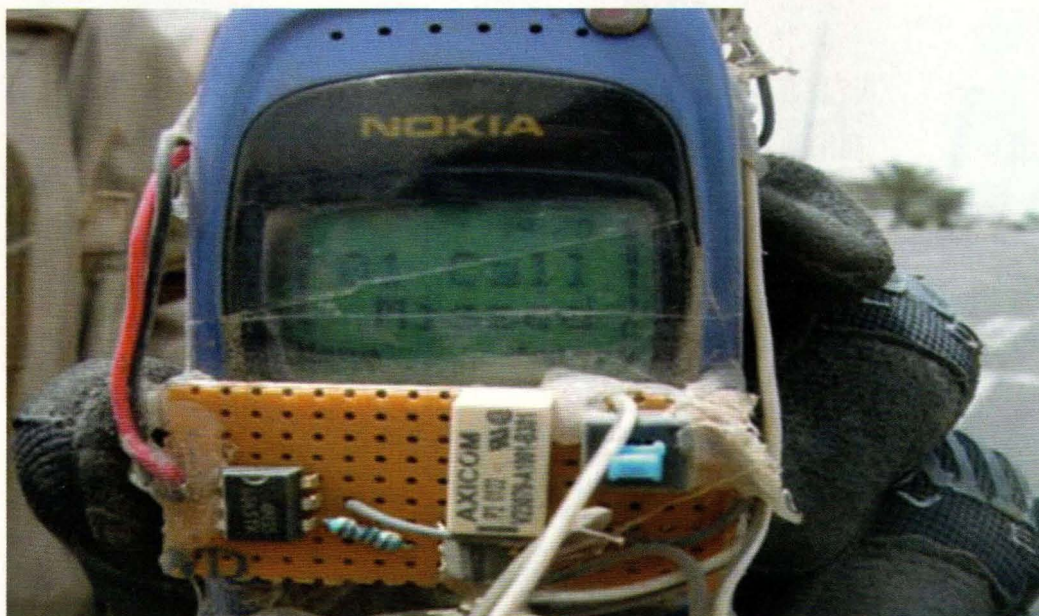
tightly gripped hands, hands rigidly in pockets pressed firmly against the torso, hands remaining inside of bags all indicate the possible and imminent detonation of a device. Wires, batteries and switches may also be seen inside of open bags or held in the terrorist's hand. These should not be confused with the covert pressel (switch) of a surveillance operators covert radio, often held in the hand on the end of a pink wire! A vastly increasing number of covert surveillance operators are now being infiltrated into public environments to conduct supposed covert counter-surveillance. However, if such operators are truly professional surveillance



Armed police in London

officers in a fully undercover counter-surveillance role, they will be utilising the concealed wireless and Bluetooth technologies that are now commercially available, in order to reduce any risk of miss identification as a suicide bomber and spark off an embarrassing alert. The public are educated more than at any other time in our history, and they too are competent in noticing unusual behaviour, we all have a "sixth sense" to some degree. Surveillance officers can become fixated too on their subjects and ignore the issue of what's known in the trade as 'Third Party Comprise' (CPT), and in a very weird twist actually adopt the same profile of the potential bomber they are surveilling. The need for more fully competent and trained surveillance officers is now more paramount than ever.

Suicide bombers will become fixated in the seconds before detonation, often walking purposefully ignoring all that is around them, characterised by blank staring faces with wide open eyes. No amount of training at a terrorist camp or clandestine detours from religious beliefs can fully suppress the extreme emotions in the seconds before perceived martyrdom. That applies to other terrorist organisations opposed to political rule, for example, such as the suicide bombers of the Tamil Tigers in Sri Lanka. It is here that a profiler, security guard, protection, police, government or surveillance officer in



"1 MISSED CALL" - US Army intelligence photo showing a terrorist cell phone detonator. Recovering items such as this has provided much useful intelligence in constructing countermeasures - and leading authorities to those responsible for its manufacture.

COURTESY: DOD

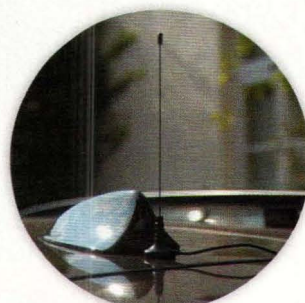
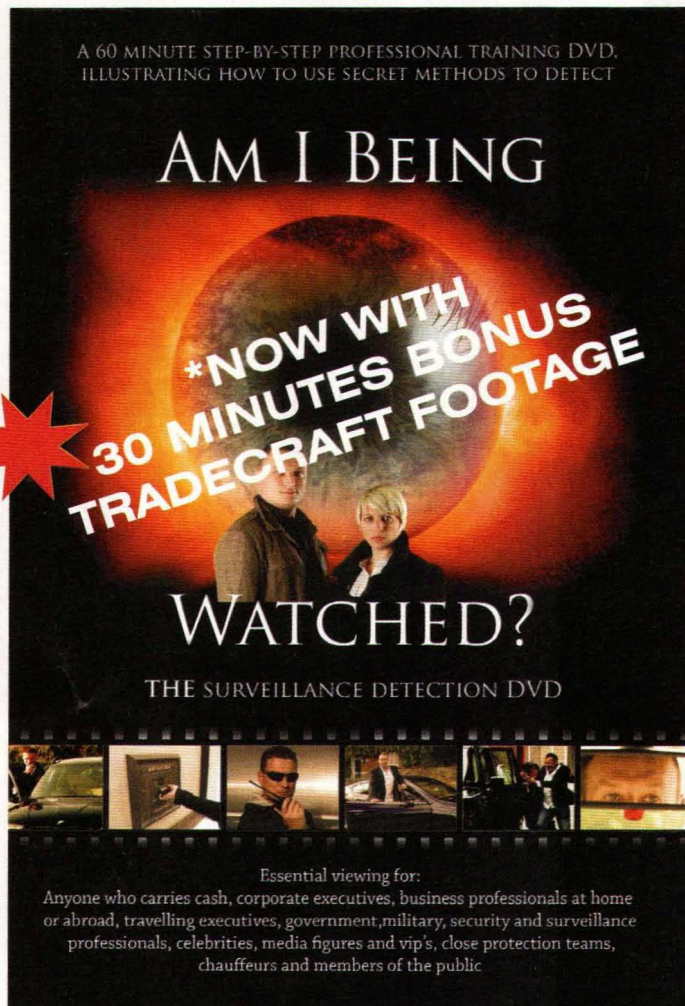
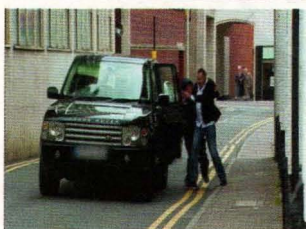
FILMED ENTIRELY IN
SUPER HD

AM I BEING WATCHED?

ESSENTIAL VIEWING

A 60* minute step-by-step professional training high-definition DVD illustrating how to use secret methods to discover...

for government, military, security and surveillance professionals, close protection teams, media figures, corporate and travelling executives, business persons, chauffeurs, celebrities and importantly - members of the public



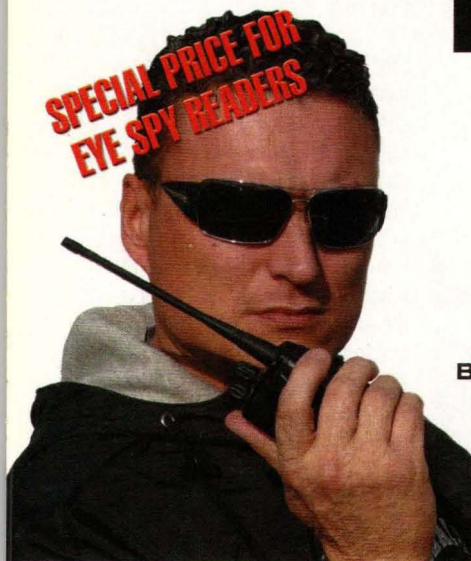
Before an attack, theft, kidnap or an attempt to gather information about you, your family, business, home or office, one thing is proven... your routine will be watched.

Learn all the secret skills used to identify surveillance without anyone knowing you are even looking... this is the art of anti surveillance.

In this highly informative, instructional and professional DVD, ADRIAN RADFORD, a former British intelligence instructor presents some of the secrets of this essential guide to discover if you are being watched

Each DVD contains discount (£5.00/\$10.00) voucher for Volume II

Am I Being Watched DVD - EYE SPY Special Reader Offer: UK £39.99 • USA \$79.99 • ROW £45.00
Usual Price: UK £49.99 USA \$99.99 ROW £55.00 WORLD
Ref: DVD-ES1 please use order form on page 82. Overseas orders sent air mail



Am I Being Watched - is part one of a professional three DVD series on anti-surveillance, countersurveillance and related tradecraft and security issues. It is produced by BLACKChrysalis and distributed solely by Eye Spy Publishing Ltd. Outlets should contact Eye Spy for trade questions and reselling licences.



pursuit of such a suspect can potentially intervene preventing the not so inevitable outcome.

If a suspect is distracted even for but a few seconds, they will not be focused on being detected or stopped, they are instead reflecting on their last moments of their life. Therefore a last minute "soft" intervention may be all that is required to "off-balance" any bomber, and in those final seconds once distracted, an explosive use of physical force can be made to render the bomber incapable of detonating their device. Any initial aggressive intervention may result in an immediate detonation, unless the use of lethal force is an option incapacitating any suicide bomber immediately. Where no firearms team is present a non confrontational distraction may lead to a successful disarmament, in some cases this will be the only chance of preventing a catastrophe.

Eye Spy: If the profile of a terrorist is indeed changing, is prevention conceivable, especially with such an evolving threat?

AR: In order to have the confidence to intervene in the final stages of any attack, education and training in realistic scenarios is perhaps the only way to practice intervention and should be included in conflict management and suicide scenarios.

Perhaps the best form of intervention is prevention through early detection, and this involves intelligence collection. The use of fully professional covert counter-surveillance teams dubbed 'Counter Terrorism' or 'CT Operations', is the most effective way of ensuring early detection is made. Adoption of such practices has historically identified and prevented some suicide attacks and terrorist attacks, along with the extensive use of CCTV and profilers. Being able to follow a suspect will allow for the gathering of specific and relevant intelligence in relation to the profile of a suicide bomber. Perhaps it is the surveillance officers who should be re-trained in terrorist profiling, with surveillance officers as opposed to close protection officers and guards being engaged in counter-terrorism activities, after all, such activities are actually a diversification of counter-surveillance.

Counter-surveillance cannot protect everyone everywhere, this is where the use of professional covert anti-surveillance drills will identify anyone conducting hostile reconnaissance against you, a high profile personality, a home, office, hotel or event location. The DVD series 'Am I Being Watched' has been developed especially for this purpose. It is the single best tool to educate anyone in how to conduct covert anti-surveillance in order to identify terrorist surveillance before they strike. Of course further anti surveillance training is fully recommended for those at a significant risk from hostile surveillance or kidnap.

EYE SPY 62: Adrian Radford continues this series of interviews on the detailed and evolving



Suspected al-Qaida suspects arrive in court overseen by a heavy counter-terrorist presence

subject of Counter Terrorism and Prevention, where he looks at how to identify those areas of vital ground that any terrorist must dominate and reconnoitre in order to successfully plan for a terrorist attack, and how to prevent them!

Adrian Radford is a senior instructor at the London School of Surveillance which offers specialist security training courses in "how to conduct successful Counter Terrorism operations" and "Counter Surveillance" for surveillance officers, guards and security specialists. Anti Surveillance courses are available on a group or 1-2-1 basis and can be taught anywhere in the world. These and other courses have recently been accredited at Level 4 by Edexcel, the highest level of accreditation ever received for a surveillance course. The London School of Surveillance BTEC Diplomas are internationally recognised qualifications. For further information please visit: www.BLACKCHRYSALIS.com



MIRROR OF MUMBAI



URBAN WAR

Terrorists strike again in the centre of a major city, as intelligence chiefs admit al-Qaida and its associates have chilling new operational agenda

Security services across the world, especially those based in major cities, are re-examining their counter-terrorist procedures following another ferocious urban terrorist attack. Masked gunmen ambushed a small convoy carrying the Sri Lankan cricket team and match officials to the Gaddafi Stadium in the Pakistan city of Lahore. Six police officers and two civilians died. Ironically, the Sri Lankans were only playing because the Indian team had decided not to play because of the terrorist attacks last November in Mumbai.

In a carefully coordinated operation, the convoy was attacked at 8.55am on 3 February, just 800 yards away from the ground. As the coach navigated the city's huge Liberty

Roundabout [circle], two cars pulled in front of the coach causing traffic to stop. The police assigned to protect the team were immediately targeted by the gunmen. Rocket-propelled grenades were fired and automatic rounds sounded for nearly 20 minutes. Several hand-grenades were also thrown at the vehicles. The gunmen were joined by colleagues who had been waiting in the area - on rickshaws.

The terrorists moved in from four directions. Five officers, only lightly armed, were killed immediately. This left the buses virtually defenceless and they were subsequently sprayed with bullets from AK-47s. Another policeman was shot and injured. A terrorist was filmed walking up to him - what happened next could be likened to an execution.

Most of the gunmen carried rucksacks filled with hand-grenades and additional bullets. However, there were "rations of food" and "high-energy" drinks in others. Some of these were recovered by police as the terrorists emptied the bags. Investigators have speculated the intention was to take the

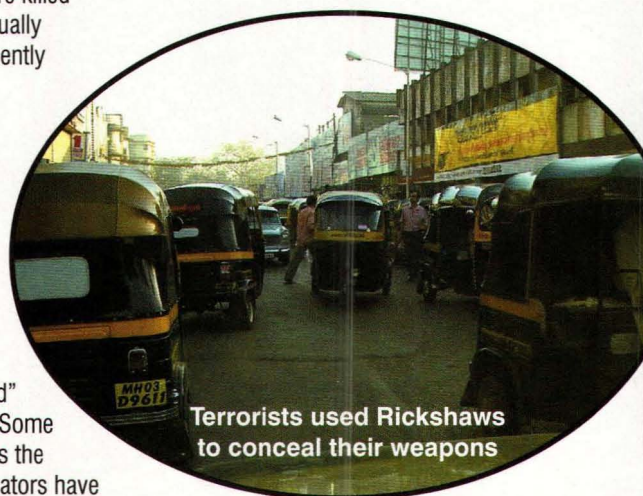


Most of the gunmen used AK-47s

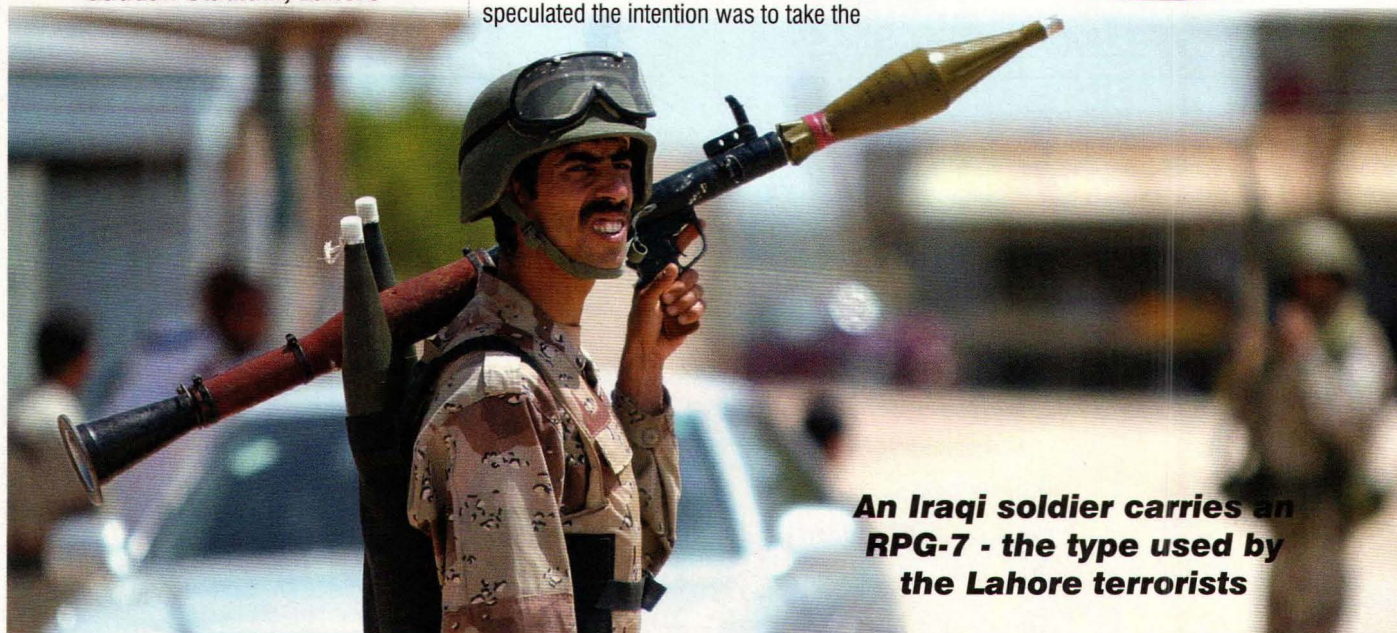
cricketers hostage. Indeed, some of their actions indicate this was the case. For example, the coach's wheels were shot at first; an RPG-7 shell was fired over its roof -



Gaddafi Stadium, Lahore



Terrorists used Rickshaws to conceal their weapons



An Iraqi soldier carries an RPG-7 - the type used by the Lahore terrorists

COURTESY: US ARMY

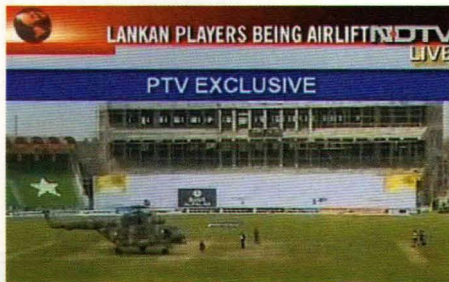
ARE



RPG-7



Two brazen gunmen attack the police security vehicle assigned to the convoy



A Pakistani Army helicopter airlifts the Sri Lankan cricket team from the ground

perhaps a warning shot -and moments later a stun-grenade was tossed under the vehicle. A gunman then shot through the windscreen. All these factors seem to suggest that the terrorists wanted to immobilise the vehicle. However, they did not count on the speedy thinking of the bus driver who accelerated away. The mini bus driver carrying match officials was not so lucky, he was killed.

"The gunmen targeted the wheels of the bus first and then the bus itself," Sri Lankan cricketer Mahela Jayawardene said. "We all dived to the floor to take cover." The driver of the team coach, Khalil Ahmed, said: "As we approached the city's Liberty Roundabout, I slowed down. Just then what seemed to be a rocket was fired at my coach, but it missed and I think flew over the top of the vehicle. Almost immediately afterwards a person ran

in front of the bus and threw a grenade in our direction."

The gunmen, aged between 20 and 30 years, operated as two-man teams - something which intelligence officials said was identical to Mumbai. Once they had carried out the raid, they retreated to the busy commercial and shopping parts of the city. Astonishingly, no arrests were made at the scene.

Anti-terrorist police found two vehicles used to stop the convoy close to the scene.

Governor of Punjab, Salman Taseer said: "These [terrorists] were fully trained people, the way they were running and the kind of weapons they had... they are the same people who launched attacks in Mumbai. They were no ordinary terrorists."

It seems probable that, based on the sophistication of the operation and the manner in which it was performed, those responsible were highly trained. Few doubt it was the work of an al-Qaida franchise group, probably members of Lashkar-e-Taiba (LeT). Pakistan police have arrested several key terrorists from this group in relation to the Mumbai attacks. "It seems pretty clear this attack was in response to the arrests and the general clampdown by the authorities in Pakistan," an intelligence source said.

Taliban militants as well as other Kashmiri jihadi groups are also in the frame. Some intelligence analysts even believe the attack could have been conducted by forces friendly to the Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka. In the past few months the army has virtually wiped out the terror group and reclaimed huge areas once occupied by the Tigers.

Intelligence chiefs now fear the "urban warfare methods" of Mumbai are being duplicated to deadly effect by terrorist planners, who have

COORDINATED AND PROFESSIONAL

Lahore police chief Habib-ur Rehman and Punjab Governor Salman Taseer (pictured) say the incident was similar to the Mumbai attacks on 26 November 2008.

"I want to say it's the same pattern, the same terrorists who attacked Mumbai," Taseer said.



Khaled Farooq, the chief of police in Punjab province agreed: "The attack resembles the Mumbai attacks. That was also a commando action and this is also a commando operation. They were trained terrorists and they attacked in a planned manner. The attackers looked like Pashtuns."

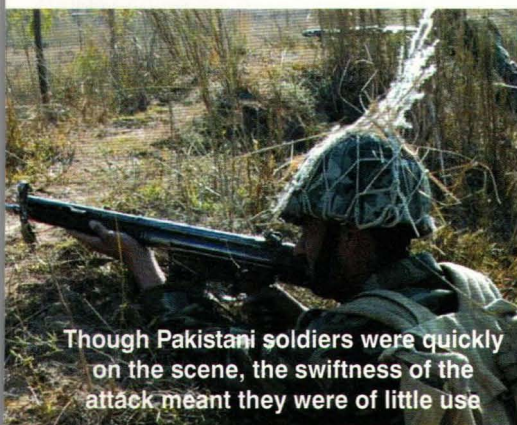
Pakistan-based elements including Lashkar-e-Taiba (LeT) have been blamed for the Mumbai atrocity.

• Former Pakistan cricket captain and now politician Imran Khan, criticised the level of security afforded to the Sri Lankan team. "This was one of the worst security failures in Pakistan," he said. "The Pakistan government guaranteed the Sri Lankan cricket team that they would provide them security."

changed their modus operandi in recent months. Al-Qaida has realised that city-centre operations can be performed using "hit and run" tactics, that are difficult to combat. In the US, senior intelligence and security figures have warned that a "Mumbai-type" attack is not beyond the realms of possibility in a major American or Western city.

As for events in Lahore, intelligence watchers were amazed that although this was the third day of the match, the coach had taken the same route on every occasion, and at the same time. Similarly, with the stakes so very high in respect of terrorism, only a lightly armed detail was assigned to the convoy.

However, much of the evidence suggests the terrorists had inside knowledge...



Though Pakistani soldiers were quickly on the scene, the swiftness of the attack meant they were of little use

© TARIQ/IMAGES

100 YEARS OF MI6 Secret Service Bureau MI5 1909 2009



This year Britain's two premier intelligence services celebrate their 100th birthday. Eye Spy steps back in time to examine the origins of MI5 and its sister agency - MI6, plus a few significant moments and characters in the journey of these organisations.

the SECRET SERVICE

British intelligence is usually traced back to Queen Elizabeth I's secretary of state Sir Francis Walsingham. In the 16th century he despatched dozens of undercover agents to seek out Catholics plotting against the throne. About 90 years later, in the reign of Charles II, regular monies were put aside for a 'Secret Service Fund', evolving later to an annual Secret Service Vote in Parliament. The monies were supposed to have been used as payment to British informants who spied on the country's enemies both at home and abroad. It later transpired that

about half of it actually fell into the hands of dubious politicians who used it for bribery and other underhand tactics. Despite this, Britain was receiving extremely useful intelligence from its overseas spies who had begun infiltrating political groups, European governments, royal families etc. The operation was described as "the long arm of British covert influence".

Many great things emerged under the rule of Queen Victoria, the Industrial Revolution for one, and you might be forgiven in believing the secret services would have blossomed also, but the exact opposite occurred. During her reign, the



*"the long arm of
British covert
influence"*



"This most rabid demagogue can say in this free country what he chooses... he speaks not under the terror of an organised spy system..."

Charles Dickens

use of agents and skulduggery to obtain information inside the UK was rare, primarily because Britain was secure and almost a third of the world map coloured a deep shade of pink. The position was virtually the same abroad and intelligence collection rare. Reflecting on this situation and the burgeoning power of Britain and its people, the great Charles Dickens wrote: *'This most rabid demagogue can say in this free country what he chooses... he speaks not under the terror of an organised spy system.'*

SPECIAL IRISH BRANCH

Dickens was of course correct, but by the end of the nineteenth century Britain's navy and army services began to note the 'rumblings' of possible conflict all over the globe. In an effort to

bolster tactical and strategic intelligence gathering, the services established intelligence divisions, though they were not secret. Much of the intelligence they gleaned came via open sources, newspapers, publications, meetings and from the notes of their respective officers when travelling or operating abroad. Other information came from representatives at Britain's vast network of foreign embassies and trading companies dotted across the globe. At the same time, in 1883, Scotland Yard established the Special Irish Branch in response to several Irish Fenian bomb attacks. This soon became known simply as the Special Branch. There were two "rebellious" countries in the British Empire where Special Branch operated its shadowy network of spies and informants - Ireland and India.



Queen Victoria had a great dislike for under-the-counter intelligence gathering... but her views were not shared by others

COMMITTEE OF IMPERIAL DEFENCE

When the Boer War of 1889-1902 erupted, and reports started to emerge of Germany's expanding military and industrial might, those in charge of analysing and combating such issues were left grasping for information. It revealed the massive shortcomings of Britain's inadequate intelligence collection ability. This led to the creation of the Committee of Imperial Defence in 1905, and the country's intelligence activities

© SNAPPERJACK OF LONDON

**GREAT SCOTLAND
YARD SW1**
CITY OF WESTMINSTER



Scotland Yard's original headquarters near Parliament

was soon on the agenda. The armed forces held joint conferences in 1906 and 1907 and acknowledged the situation was at best poor, at worst dire. However, the Foreign Office disliked the notion of spying, describing it as "ungentlemanly and underhand". As for the notion that a home-based secret service be formed to identify subversives and foreign spies, this was seen as being against Britain's "liberal traditions". Yet there were those in Whitehall who recognised the need to construct and put in place (at the very least), a competent and secure mechanism to gather information. One man who was tasked with lobbying for change was Lieutenant Colonel James Edmonds. He had participated in the Boer War, which from an intelligence perspective, had been a dreadful affair. Edmonds, however, had run a successful unit called Section H - which examined (and censored) cables and mail flowing in and out of South Africa. Unbeknown to Edmonds at the time, he was actually laying the foundations of Britain's Security Service - MI5.

MILITARY OPERATION 5 (MO5)

In 1907, because of his experience, Edmonds was selected to join MO5 - a specialist, but tiny element within the War Office Directorate of Military Operations. George MacDonogh headed the section, which besides its counter-espionage activities, was also responsible for protecting ciphers and the censorship of post and telegrams. Also involved was Sir Walter Kirke, who worked under MacDonogh and who has been credited with helping to establish the Intelligence Corp prior to WWI. An archive document written by Kirke, notes that MO5's CE (counter-

espionage) unit was headed by Major Vernon Kell. Kell was effectively head of MI5 from its inception in 1909 until 1940. MacDonogh also controlled the activities of a certain Captain Mansfield Cumming (Royal Navy), who would later emerge as the chief or 'C' of MI6 ('C' standing for Cumming - not chief). MacDonogh was also close to Lord Curzon who would chair the War Cabinet Committee. (MI5 would later site its headquarters on Curzon Street in London).

One of Edmond's first tasks was to put in place several operations aimed at assessing the spy threat posed by Germany. His conclusions stunned Whitehall and moves were afoot to strengthen domestic security - especially against

German spies who were seemingly everywhere. The "liberal" values of Queen Victoria's Britain were slowly being replaced by nationalism and xenophobia. This was reflected in the media who warned about large numbers of German spies in



German General Headquarters, General Paul von Hindenburg, Kaiser Wilhelm II, General Erich Ludendorff. Left: A French postcard depicting the Kaiser as a war monger



BUILDING BLOCKS OF THE BRITISH SECRET SERVICE

L-R: Lords Curzon, Sir Mansfield Cumming and Vernon Kell



COURTESY: THAMES HOUSE/MI5

Britain, the Kaiser's growing and impressive navy, and a secret army that had been put in place to rise against the UK at a moment's notice. Lord Northcliffe's *Daily Mail* led the charge of alarmist reports and even published Germany's "invasion plans". The *Mail* was not alone, a letter in April of 1907, written by an army colonel in *The Globe* read: *The Streets of London swarm with Germans... where do they go? They are comfortably dressed and well nourished... they are undoubtedly soldiers.* There was even a report that reached Whitehall suggesting German soldiers were operating as waiters in restaurants, a notion dispelled by Edmonds. Yet as we shall see, Edmonds had seemingly fallen for the paper talk. The grumblings of his peers that spies were walking London's streets and alleys, and being sent to its docks and ports to spy on its ships, convinced Edmonds there was some substance in the reports.

SPY RINGS IN LONDON

All of this was hysteria, of course, but the outcome was a serious and fresh look on how Britain should position itself when dealing with global and domestic security matters. And this at a time when its Empire was being threatened by an ever-growing, dominant and powerful Germany. However, and bizarrely for a man like Edmonds, he ultimately concluded in a report to the War Office, that a vast underground network of German spies was indeed "roaming the countryside" and being operated centrally from the capital.

His report ended up on the desk of Major General Spencer Ewart, the Director of Military Operations, essentially Edmond's superior. Ewart was angry at the report, not because he disagreed with its content, but because he wanted to establish his own network of spies in Germany. If emphasis was placed on counterespionage, his plans for a foreign intelligence collection service, could be set back. Ewart then played a master-stroke. He announced that the only way to compensate and support both objectives, was by creating an organised secret service bureau and strengthening the Official Secrets Act. At this

moment lay the origins of Britain's modern intelligence services.

Not everyone agreed with Ewart, including the Secretary of State for War, R.B. Haldane. But shortly thereafter, in 1909, came the "timely" writings of a certain William Tufnell Le Queux (above right).

The Weekly News ran a series of features that swelled public opinion that spies were everywhere. Le Queux's stories - 'The Spies of the Kaisers' featured fictional heroes and story-lines not unlike those that Ian Fleming would scribe decades later on the activities of a certain "James Bond". Staggeringly, this prompted the government to act, primarily because of the public support for Le Queux, who was starting to mix a little fact with fiction. *The Weekly News* was a much sought-after publication, and with a tantalising 'reader offer' of £10 to any person who could identify a German spy, the reports of spy activity increased. Men with wigs, Germans with maps (tourists) foreign cars, people dressed with German-made suits, all came under suspicion. And god forbid if you had a foreign accent or were seen near a pigeon.

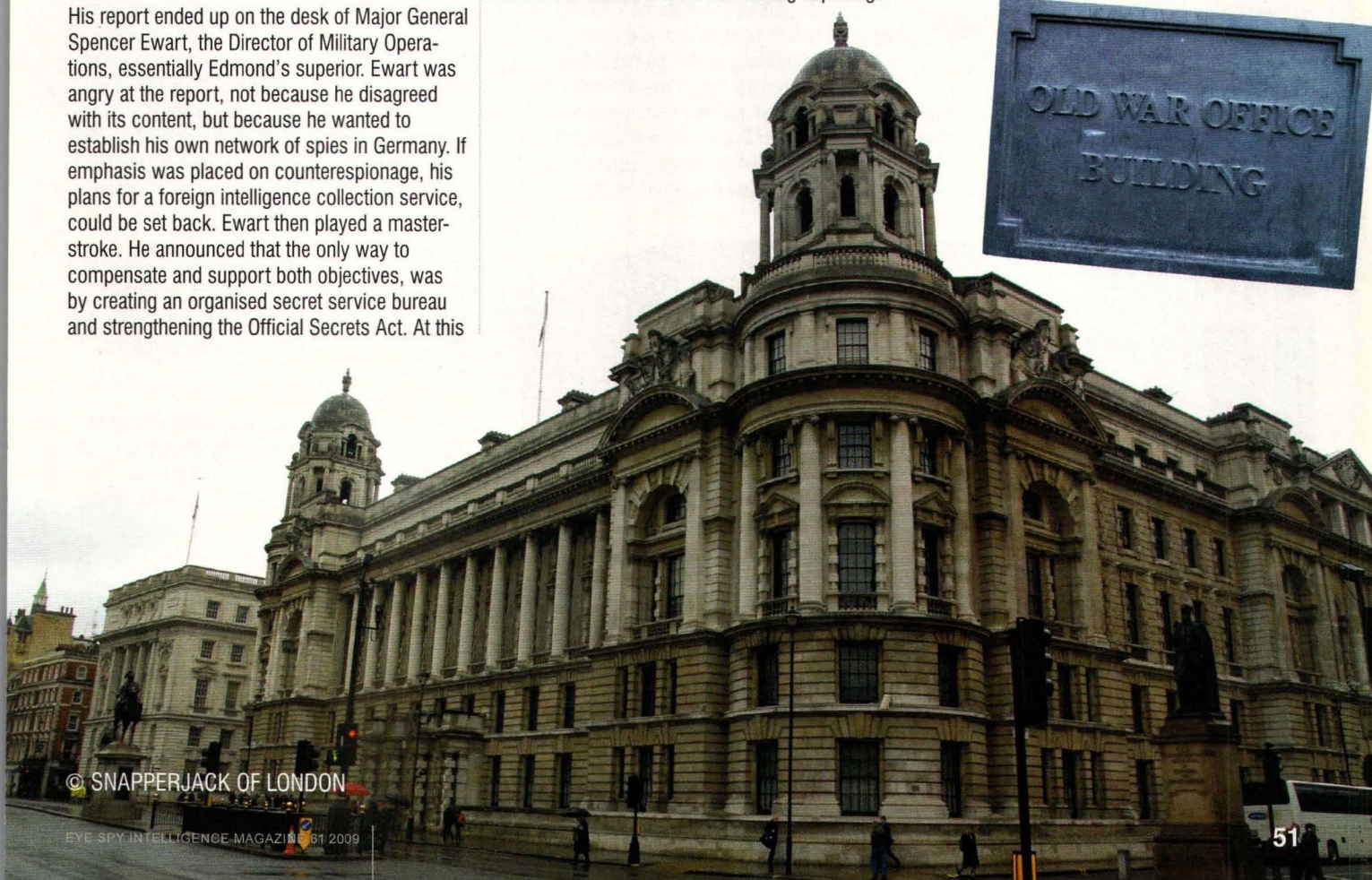
SECRET SERVICE BUREAU

The Committee of Imperial Defence discussed the "rampant spying", but was not totally convinced by Edmond's report. It did, however, believe the Germans were conducting espionage

and that the Kaiser had authorised a plan to invade Britain to be drawn up. In July 1909 a sub-committee recommended that police be given more powers to question aliens and prevent sabotage. Yet its most important decision was to agree with Ewart - a move post haste towards establishing the Secret Service Bureau - SSB.

The plan was for the SSB to be a single entity engaged in both domestic and overseas intelligence activities. But by 1910, it seems the Bureau was already beginning to separate. Officials opted to form a military and naval section. The military section would have domestic and overseas arms - basically a security service engaged in counter-espionage, while the naval section would help create Britain's network of foreign agents and run collaborators.

Sir Vernon Kell, who had to resign his army position because of the new model, designated MO(t) as the actual name of his counter-espionage organisation. The operation was run from a single room in the War Office with an incredibly low budget of just £7,000. One of his first tasks was to create an 'alien register' by gathering and researching the names of some 30,000 UK-based Germans. He also started investigating Le Queux's theory that the Germans had established a major spy network in southern England. He obtained the cooperation of police forces and by 1914, the year when war would explode across Europe, MO(t) had details of



ARRESTED AS GERMAN SPY.

Kaiser's Army Officer Held Without Bail by English Authorities.

PLYMOUTH, England, Aug. 19.—Philip Max Schultz, a German army officer, was arrested here to-day, charged with espionage. It is alleged that a mass of incriminating correspondence was found in his possession.

Bail was refused, and Schultz was remanded by a Magistrate for one week. The prosecution intimated that the German Government was involved in the case. The prisoner is a Lieutenant of the Thirtieth Hussars, stationed at Frankfurt-on-the-Main.

A US press report from 20 August 1911, concerning the arrest of Max Schultz

COURTESY: NEW YORK TIMES

11,000 Germans. Kell's operation was of course doomed before it began, because there was no credible national spy network and the Kaiser did not have a viable and concrete invasion plan.

Despite this, Kell had already uncovered a German navy spy ring which operated on the south coast via contacts in London.

In 1911, MO(t) had become aware of a German journalist, Max Schulz, who lived on a houseboat in Exeter. He was sending reports on the Royal Navy to a Gustav Steinhauer, a former detective of the Pinkerton Agency and one-time bodyguard to the Kaiser himself. The correspondence was sent to addresses in London where it was forwarded by German contacts to a bogus address in Potsdam c/o Steinhauer. Kell became suspicious and probed deeper. Schultz's mail was opened and copied by General Post Office (GPO) specialists (see Eye Spy 58 Dollis Hill). And though they discovered everything Schultz was writing appeared open source, the addresses of the 'middlemen' and contacts soon put Kell's officers onto the Kaiser's agents. Heinrich Grosse was arrested working as a stoker on board the Royal Navy destroyer HMS Foxhound and Dr Armgaard Graves near the dock yards in Glasgow. Kell was careful not to let details slip out into the media and thus alert the

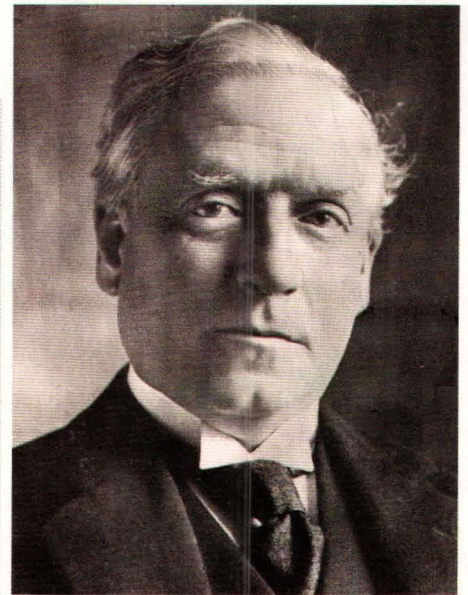
rest of the Steinhauer spy ring. The end game to this operation, which was effectively 'MI5's' first successful counter-espionage activity, came about with the arrest of Royal Navy gunner George Parrot in November 1912. It transpired that the man who had recruited Parrot, a certain Karl Hentschel, had tried to blackmail German intelligence after threatening to reveal Parrot's role to the British. Kell was alerted and gave Hentschel £30.00 to tell everything he knew about the spy ring - which he promptly did.

Kell's agency was gaining credibility and a reputation in Whitehall and beyond. And despite the incorrect assessment on the "huge network of spies", it was of some importance that when war broke out, Kell's intelligence, due to the earlier surveillance operation, was central to the detention of about 200 "undesirable Germans" and 22 suspected agents. As it later transpired, only one of the 22 people was charged with espionage. He was a hairdresser based on the Caledonian Road. Acting as an agent, the man had been forwarding mail to Steinhauer for a fee of just £1.00 per week.

Prime Minister Herbert Asquith was delighted and visited Kell at his office. On the wall Kell had prepared a somewhat dubious map highlighting where the German spies were based in the UK. This too impressed Asquith who said it was a "major victory."

SPYING - "A CAPITAL SPORT"

Britain's Security Service was up and running. Meanwhile, the foreign intelligence collection arm of the Secret Service Bureau, now designated MI-1(c), had chosen 50-year-old Commander Mansfield Cumming as its first head. Cumming had been retired from the Royal Navy for 20 years. A constant sufferer from sea sickness meant his career in the navy was affected, but he had proven himself useful in intelligence matters. He spoke of his new position to colleagues as



Prime Minister Herbert Asquith - "delighted" with first spy arrests

"exciting" and described "espionage" as a "capital sport."

Unbeknown to many in the intelligence world, Cumming's office in Whitehall Court could only be accessed by a series of bizarre openings. He had built a mechanism of levers and peddles which he himself controlled. Once pressed, a false wall would open revealing a hidden staircase to his office!

Writers have long noted his eccentricity, and the man who often wore a monocle and only wrote in green ink, would add another chapter to this legacy after a car crash near Paris in 1914. Cumming was driving with his son and crashed into a tree at high speed. His son was flung from the car and fatally injured. Cumming could not reach his boy because his own leg was trapped and badly crushed. According to one report, he calmly took out his penknife and started to chop away until he was free. He then reached over and put a coat over his dying son. The report of his "penknife bravery" has been rejected by many researchers, but his new wooden leg was definitely something of a talking point in Whitehall itself. Cumming had a tendency to tap his new appendage with a knife much to the puzzlement of others. It was also, apparently, not unusual for him to be seen dashing about the corridors on a child's scooter.

Outside his office, Cumming became known for donning disguises and terrifying the public as he drove particularly quickly and dangerously through the streets of London in his Rolls Royce.

THE ADMIRALTY

MI-1(c), unlike MO(t) was placed under control of the Admiralty, which traditionally had been the dominant organisation in intelligence collection. A year after MI-1(c)'s formation, two navy officers, Captain Trench and Marine, Lieutenant Brandon, were arrested by Germany for spying. And though they were operating under the auspices of the Admiralty, not Cumming's MI-



Caledonian Road, London - scene of the first capital spy arrest by the fledgling MI5



Cumming's first office in Whitehall Court could only be accessed through a false staircase - controlled by the head of MI6 himself using levers and pulleys

1(c), it was a wake-up call for Cumming that the great game was one not to be taken too lightly.

By 1910, Cumming had started to enlist the occasional support of travelling British businessmen, industrialists, arms dealers and others to help gather information. This was particularly successful in Europe, especially Rotterdam and Brussels. Both these locations would play a significant role in the development of Britain's Passport Control Officer (PCO) spy network (see Eye Spy 60). But the fledgling Service still had a lot to learn. For example, in Brussels, Cumming's men were offered a "secret German codebook". They requested permission to buy the book for £600.00 - a sum duly paid by MI-1(c). To Cumming's shock, the book turned out to be a forgery.

With war looming, at least Cumming had some "agents in place" at the edge of what would be a huge battlefield on the Western Front.

THE DETECTION BRANCH

By this time, Kell's MO(t) had had a name change to MO(g) and one year into the war (1915), it was officially renamed MI5 (Military Intelligence 5). Kell's staffing levels had also increased from just 14 operatives and a tight budget of just a few thousand pounds, to 850 and a 'war purse' of £100,000. Besides operating in the UK against possible German spies and collaborators, MI5 operated the Military Port Control Service - checking on all the comings and goings

(see the 'Alien Registry'). Agents were also sent to Europe and a new section was created called the Detection Branch. Already the signs were there that MI5 had arrived and was now starting to expand rapidly.

In neutral Holland, MI5 had been providing useful intelligence on the war, until its undercover agent - a man called James Dunn of the *Daily Mail* - was arrested by the neutral Dutch authorities in 1915. Cumming's Rotterdam bureau then took over the operation to send back intelligence.

Counter-espionage activities were on-going, but the Kaiser's spies, at least those who were identified, were no match for Kell and his team. One hapless operative - Karl Lody - was infiltrated into Britain using a stolen American passport. His post was opened by an MI5 censor which showed him corresponding with a known German agent in Sweden. He was executed by firing squad in the Tower of London on 6 November 1914. He would be joined by 11 of his fellow spies as MI5 sought out German spies, at British ports, airfields and weapons factories.

Kell also had some lucky moments. The German spy Robert Rosenthal, for example. He had written a letter to his handler from his home in Copenhagen giving details of his forthcoming secret spy mission to Britain. The letter "somehow" found its way into a post bag marked "London". An inquisitive MI5 censor spotted the letter and duly opened it. A few weeks later, Rosenthal took a boat from Holland and arrived at the docks in Newcastle-upon-Tyne. Kell had been patiently waiting with his team who duly arrested the unknowing spy. And though Rosenthal agreed to provide MI5 with every assistance, including the names of other German agents, Kell was guarded because his "prize catch" was a brilliant ex-forgery and a cocaine addict.



The Tower of London. It was here German spies were held, interrogated, and ultimately executed by firing squad. Inside the building a wooden chair is still maintained... complete with bullet holes

IGNORE TALE TOLD BY SPY.

Government Takes No Cognizance of Story of Forged Passports.
Special to The New York Times.

WASHINGTON, June 6.—Until it gets a report on the subject from Walter H. Page, the American Ambassador in London, or receives corroborative evidence from other sources, the State Department will not take cognizance of the newspaper story from London that Robert Rosenthal, said to be a German spy, and under arrest as such by the British authorities, had confessed that the German Government had a perfect equipment for manufacturing American passports. Rosenthal was credited with the statement that Captain von Prieger of the German Admiralty was engaged in such a plot.

More media concern in the US about German spies - in this case Rosenthal's special gift in the art of forgery

Kell was winning his secret battle with the Kaiser's spies, and by 1916, Germany had all but given up on the notion it could glean valuable intelligence through espionage on Britain's streets. Kell, however, was still keen to surveil and build up MI5's 'Alien Register'. By the end of the war, his office had a near 140,000 files of "individuals and persons of interest".

NAVAL INTELLIGENCE DIVISION (NID)

Cumming's foreign intelligence section, meanwhile, was still playing second fiddle to two powerful agencies operating in the intelligence arena. Firstly there was the Naval Intelligence Division (NID) which was reluctant to simply allow MI-1(c) a clear run in overseas intelligence collection. Its role had become crucial following the outbreak of war. And then there was the British Army's Intelligence Corp, already playing a pivotal role in the battlefields of Europe. By 1916, MI-1(c) had been moved from the Admiralty to the War Office. It was now but one of four sections employed in the field of intelligence gathering and analysis. The War Office also ran the cryptanalytic bureau MI1(b), but the Admiralty would soon acquire a codebreaking gem of its own.

CODEBREAKERS OF ROOM 40

The NID, was perhaps the defining agency at this moment, primarily because it was best placed to control Sigint (Signals Intelligence). This was further augmented by the delivery of a German code book from the Russians, who had discovered the "gem" in the pockets of a dead German naval officer from the battleship Magdeburg. The Director of Naval Intelligence was a legendary figure known as Captain Reginald 'Blinker' Hall. Hall, recognising the clear advantage which breaking codes and secure communications offered, set about forming a section which was central in the understanding of German radio traffic. 'Room 40' of the Admiralty operated in great secrecy and played an underhand role in getting the Americans "on board" with the British in their fight against the Germans. In January 1917, a German telegram sent by the Kaiser's Foreign Minister - Arthur Zimmerman, to the German ambassador in America, was intercepted. After decoding the signal, Room 40, and ultimately British intelligence knew they had the document that would force America's hand. The note said that Mexico should be "encouraged" to join Germany and in return, it would promise a huge section of the southern United States. There was also a reference to "unrestricted warfare" which essentially meant Germany was prepared to target neutral shipping, including US vessels in the Atlantic. British foreign officials, intelligence



Arthur Zimmermann and part of the signal decrypted by Room 40 codebreakers

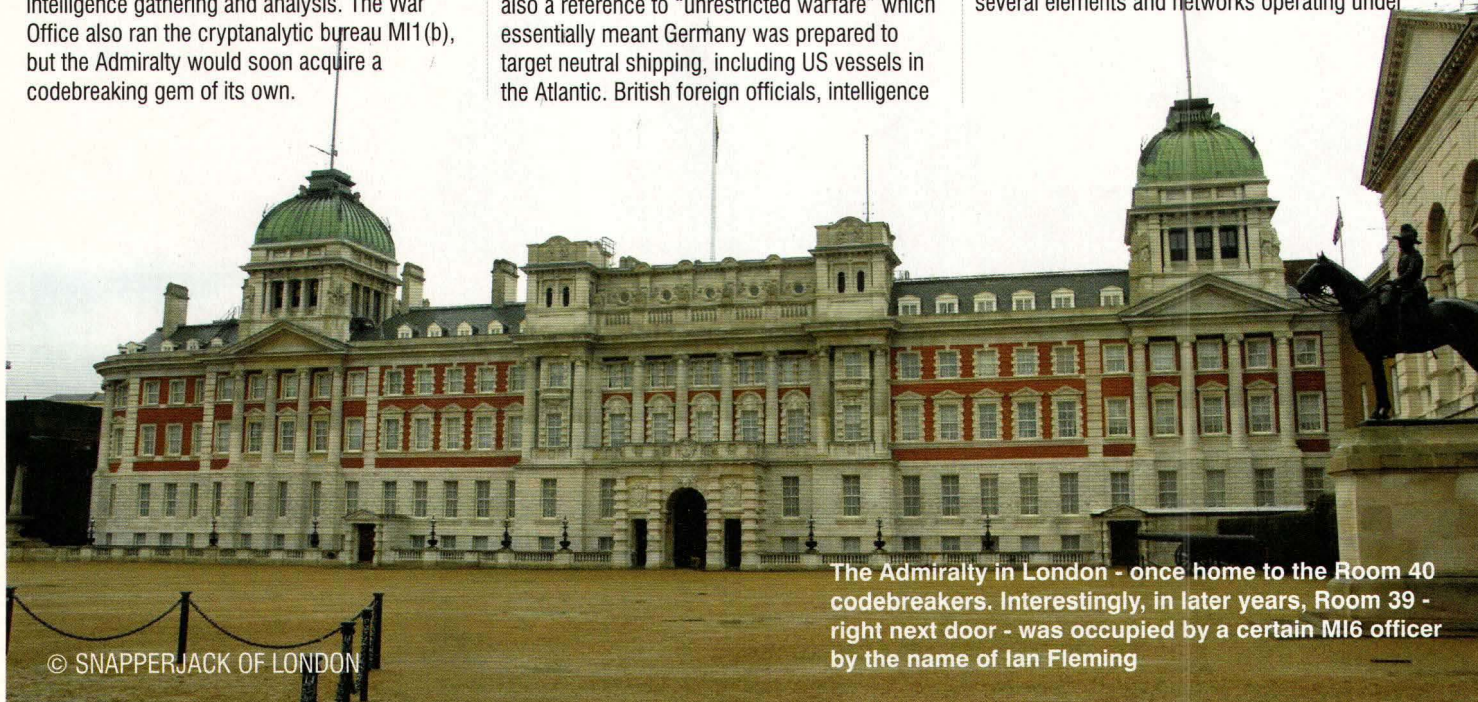
4458	geminnam
17149	Friedenschluß.
14471	○
6706	reichlich
13550	finanziell
12224	unterstützung
6929	und
14991	einverständnis
7382	ausserhalb.
156(5)7	Pa/3
67893	Mexico.
14218	in
36477	Texas
5870	○
17553	neu
67893	Mexico
5870	○
5454	AR
16102	IZ
15217	ON
22801	A



in hand, showed the document to President Woodrow Wilson, who was fuming. America, soon decided it was no longer neutral.

MI-1(c) and the Intelligence Corp had, by late 1916, developed their own spy networks in Europe. As part of the General Staff, the Intelligence Corp was charged with gathering tactical intelligence, while Cumming and his team focused on strategic intelligence. There was conflict, and relations were not good.

Undeterred, Cumming continued to carefully developed his operation and there were already several elements and networks operating under



The Admiralty in London - once home to the Room 40 codebreakers. Interestingly, in later years, Room 39 - right next door - was occupied by a certain MI6 officer by the name of Ian Fleming

© SNAPPERJACK OF LONDON



The work of Room 40 codebreakers and a little "skulduggery" by British diplomats left President Woodrow Wilson with no option but to join the war

MI-1(c). One section, code-named FRANKIGNOUL after one of its senior agents, had a dedicated team of about 30 agents who monitored train movements. But disaster was to strike and following the interception of reports from a steamer in the North Sea, the network was compromised and ten MI-1(c) agents were executed in 1917. Nevertheless, Cumming persisted and built new networks and developed existing ones, including the largest of them all - the DAME BLANCHE - originally devised by military intelligence. This 'train-watching' group numbered a staggering 1,000, and passed a variety of intelligence about troop and armaments' movement, high-profile figures seen at different towns and cities, and general intelligence. Of the 1,000 people involved, only 35 were ever arrested.

Besides the European theatre, Cumming began deploying his forces further and further afield - this laying the genesis for today's global MI6



William Somerset Maugham

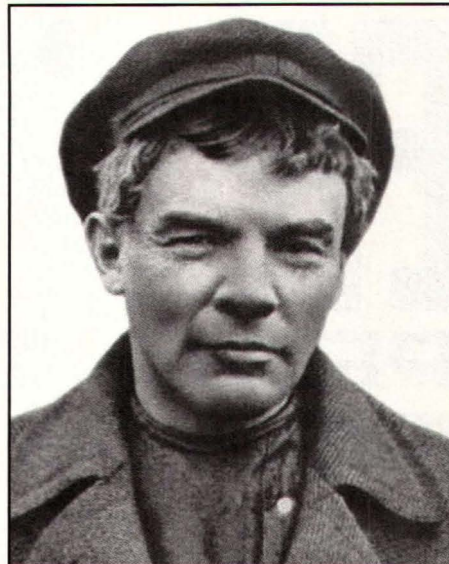
intelligence operation. This worldwide ambition had actually started quietly in September 1914. Indeed, the first office which could be described as an MI6 Field Station opened in Petrograd, Russia. Here, Cumming appointed Major Archibald Campbell with a task to augment and support Russian signal's intelligence. Typically, Cumming inserted a somewhat devious caveat... Campbell was instructed to create an underground network of his own MI-1(c) agents. However, because of Foreign Office rivalries, Campbell was soon back in the UK. Despite this, on 7 November 1917, Britain was in a position to understand and observe the collapse of her former Imperial ally to communism and the take-over by revolutionary Bolsheviks. Five months early, Cumming had sent the revered novelist William Somerset Maugham to Petrograd, in a vain attempt to help 'White Russia'. On 31 October he returned to London carrying an urgent message - a desperate appeal for arms. Downing Street replied "can't help."



MI6's Bruce Lockhart and Sidney Reilly

Britain still had an "unofficial mission" in Russia, and because the country was still an "ally", Cumming used his skill to bolster Britain's intelligence gathering ability. The mission was headed by Bruce Lockhart and he would soon liaise with one of MI6's most legendary spies - Sidney Reilly - a brilliant disguise expert and described by Cumming as a "sinister man who I could never trust." Their objective was to overthrow the new Lenin government by conspiring with the anti-Bolsheviks. The 'Latvian plot', as it was known, was aborted in 1918, and perhaps this was best for Cumming. The British intelligence officers had made contact with two Latvians of the Kremlin Guard who claimed troops were ready to take on the Bolsheviks. However, it would later transpire the men were actually agents of the Cheka - the Bolsheviks' secret police and ultimate forerunner to the KGB. There were other plots to assassinate Lenin, and one in particular forced Reilly into hiding. He eventually escaped on a Dutch freighter, while Lockhart and another officer were arrested. Both eventually returned to the UK in a very early "spy swap" involving a Bolshevik official who had been detained in London... by Kell's MI5,

By the end of World War One, Britain's fledgling MI5 and MI-1(c) had proven themselves worthy



Lenin allegedly pictured in disguise - complete with wig and minus moustache

additions to the intelligence community. Both services had played important parts in helping the allies defeat the Kaiser. Indeed, both Kell and Cumming were given knighthoods. With victory against Germany assured, MI5 was run down again, and given a paltry operating budget of just £25,000 a year. MI-1(c) fared even worse - and most of its experienced staff were lost to other departments. In 1920, MI-1(c) was officially renamed Military Intelligence 6 (MI6) to align itself with MI5's designation. The UK now operated dedicated foreign and domestic intelligence agencies. In later years, MI5 would become known as The Security Service, while in 1921, MI6 took on the official title of Secret Intelligence Service or SIS.

DIRECTORATE OF INTELLIGENCE

In respect of the running down of these organisations, things could have been even worse, of course. In 1921, the great Winston Churchill returned to the once historical notion that Britain should have a unified Secret Service Bureau. Kell and Cumming resisted, though a new service, the Directorate of Intelligence (DOI), which had been formed a year earlier, took over the responsibilities of tackling subversion in Britain. Kell eventually succeeded in convincing ministers that this was a job MI5 could do itself - without the creation of yet another service. The DOI imploded shortly thereafter, and ten years later, another intelligence arm, the Special Branch, was also absorbed by MI5.

In 1923, MI6 under Cumming, snatched Room 40 away from the Admiralty. With a plethora of skilled cryptographers, Cumming helped shape what is today known as GCHQ - Government Communications Headquarters. However, before that, Room 40 was renamed the Government Code and Cypher School (GC&CS).

Sir Mansfield Cumming had overseen the birth of a truly global institution... he died later that year. As for Kell, he would continue the development of MI5 and head its numerous directorates until 1940.

EYE SPY

PRODUCT REVIEW



PI-CAMCORDER STICK

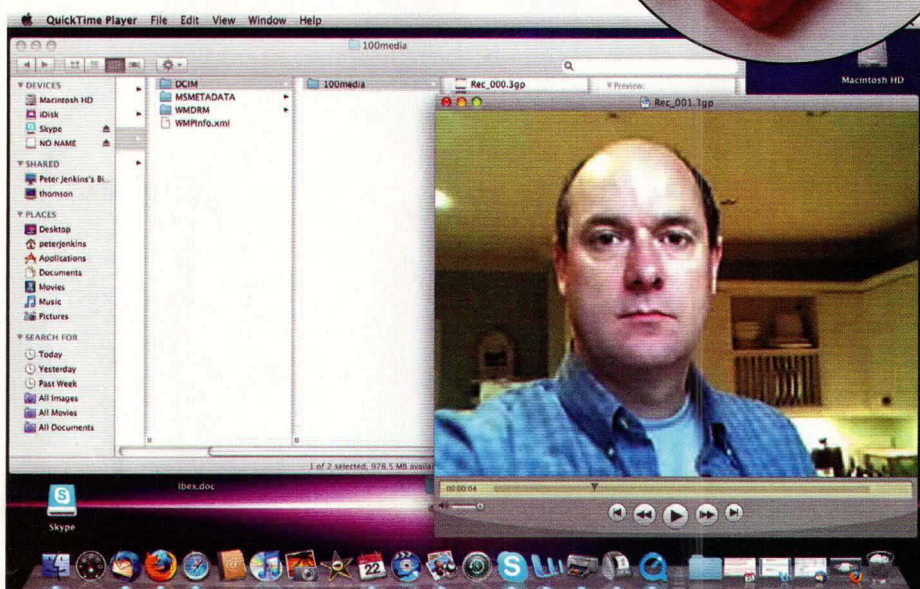
Miniature Digital Video Camera

PETER JENKINS

During a recent close covert surveillance operation, we were charged with obtaining good photographs of a target for identification purposes. There was nothing more simple and effective to use than the self-contained micro DVR - of PI-Camcorder Stick - as it is sometimes called. The trade say it is "the world's smallest high-quality camcorder", though its likely the professional services might not agree! However, the end result and quality is much higher than I suspected. Indeed, it is exceptional.

The small device measures only 73 x 20 x 11mm and weighs just 18gm. It could easily be mistaken for a lipstick holder or cigarette lighter. The camera comes with a fixed clip - ideal for placing in your top pocket. Its flat shape gives the appearance of a highlighter pen or similar.

For its price, this has got to be one of the smallest, yet top quality cameras I have seen to date.



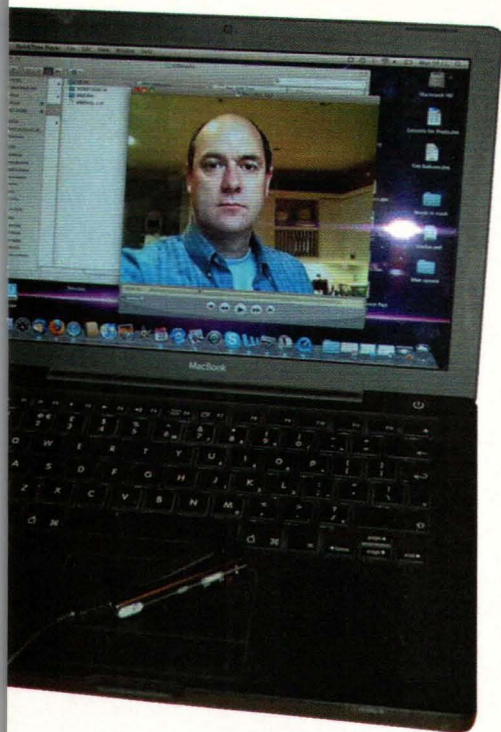
Playback quality is excellent and extremely easy to use

It is simple to operate: you slide a switch to change between still photograph mode and video mode, then just press one button to record. Press it again to switch off.

Connect the camera to a computer (Windows or Mac) with the supplied USB lead and the video files can be "dragged" across to the desktop just like any other file when using a data memory stick. The USB cable also acts as a charger for the internal battery.

There are two versions available, one which stores the images/video onto a Micro SD card, the other onto its internal 4GB memory which enables recordings for up to about two and a half hours.





The video format is 3GP (similar to MP4), which can be played back using Realtime, Quicktime or Windows Media Player. The video can also be played back on a mobile phone - if it takes the same size Micro SD card. This is really handy for reviewing the video footage before leaving a target area.

The resolution is quite high and it appeared to work well in low light although a highly lit background can make the central picture slightly dark.

A cracking simple to use mini video camera that can easily be bodyworn or concealed.

Technical Data

Dimensions: 73 x 20 x 11mm
Weight: 18gm
Video compression: 3GP Video Format, 177 x 144
Power: Internal lithium-ion
Record time: Up to two hours
Charging time: Three hours for full charge
Video file size: 500kb per minute
Memory card: Supports 128MB to 4GB micro SD
Internal memory: 4GB
Voice recording: Support voice and video
Video file: 352 288 CIF resolution
Video formats: AVI
Support system: PC and Mac
Lens: Wide angle 3.6mm lens

Unit includes: PI-Camcorder Stick • USB cable • 1GB micro SD card and SD adapter •

EYE SPY SPECIAL OFFER

**SAVE
£50.00
(\$100.00)**

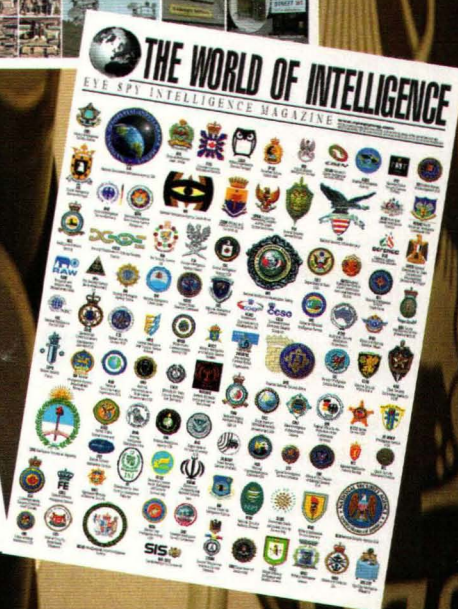
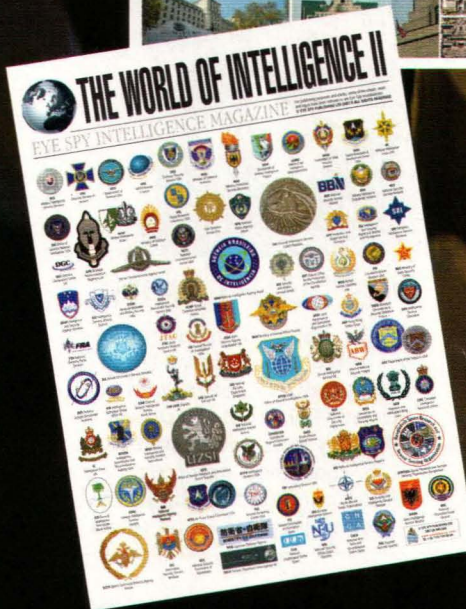
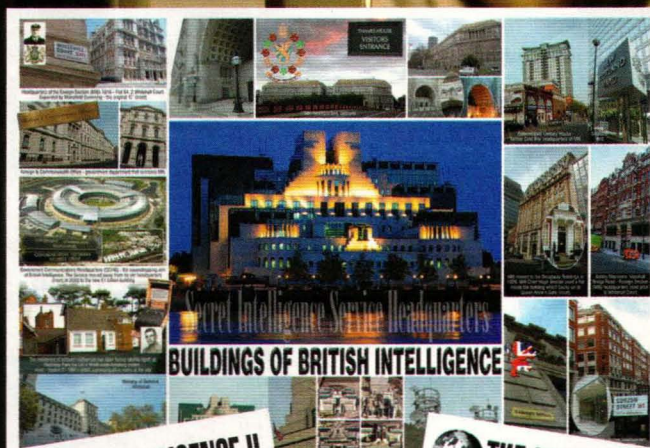
PI-CAMCORDER STICK - Ref: PIC-OFFER

UK SALE price just **£79.00** - usual £129.00
USA SALE price just **\$145** - usual \$245.00
Worldwide SALE price **£89.00** - usual £135.00

Use order form on page 82

ACCLAIMED LUXURY INTELLIGENCE POSTERS OF EYE SPY

BUY THE COLLECTION AND SAVE!



Unique gifts - suitable for framing

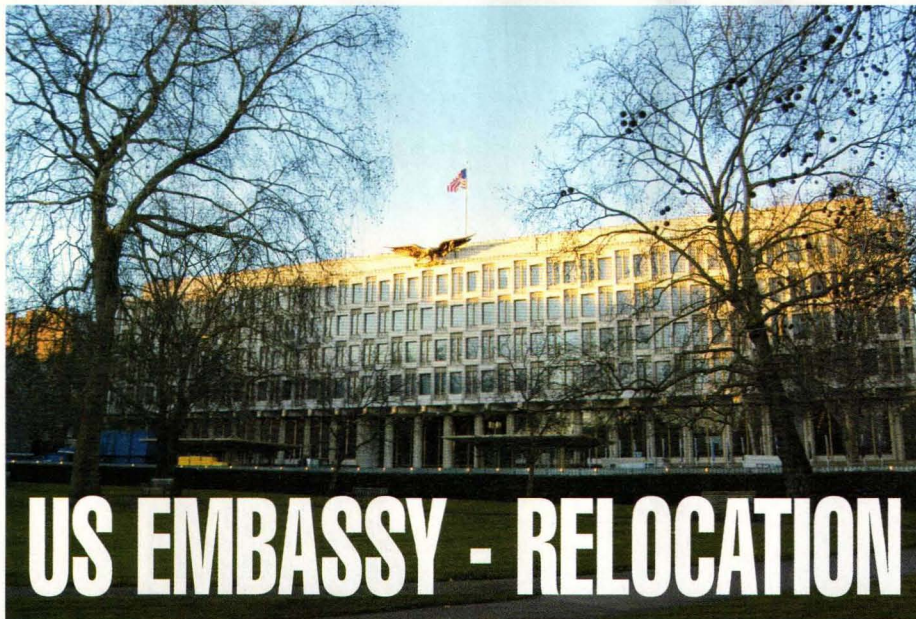


Order Ref: ICBP

UK £14.00 + £2.99 postage (Save £5.20)
USA \$29.99 + \$10.00 postage (Save \$11.00)
ROW £16.45 + £4.95 postage (Save £5.00)

BUILDINGS OF BRITISH INTELLIGENCE
A2 SIZE (841mm X 594mm)
INTEL CRESTS' POSTERS I AND II A2 SIZE
(420mm X 594mm)

COMING IN 2009 - INTEL CRESTS POSTER 3



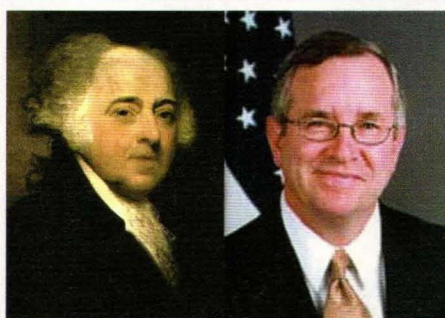
SECURITY CONCERNS FORCE AMERICAN EMBASSY AWAY FROM LONDON'S MAYFAIR AREA

For 200 years the United States has had an embassy in the Mayfair area of, London. The first ambassador was John Adams (later American president) who held the position from 1775 to 1778. However, that is about to change, as the modern impressive building which today dominates the site in Grosvenor Square, has been given its "last orders".

During the 1960s the embassy was a magnet that attracted peace protesters opposed to the Vietnam war, and more recently, demonstrators seeking to vent their fury against events in Iraq have made a beeline to the embassy.

Of course, the building is situated in a residential area of London, and since 9/11, it has been on high alert, with terrorist threats aplenty. With mounting fears, the US Government has decided to relocate to a more secure site, indeed, Washington is said to favour an area near the banks of the River Thames and quite close to the iconic 'legoland' building that is headquarters to MI6.

The ambassador, has long recognised the fears of local residents (some 100 protested and



PAST AND PRESENT

Left: The first ambassador - John Adams who would later become US President. Right: Richard LeBaron, who has served as the Minister at the United States Embassy in London since 16 August 2007, became Chargé d'affaires ad interim upon the departure of Ambassador Robert H. Tuttle on 6 February 2009.

paid for an advert regarding possible terror attacks), but was keen to stress the move was not just on security grounds. Indeed, it is not the only US embassy to seek new pastures. Following a major review of all its overseas concerns, the US government has revamped its security on many buildings, while other city-centre embassies have relocated to the suburbs.

After 9/11, the London embassy, first occupied by the US diplomatic corp in 1960, became something of a fortress with new security balustrades, fences and a security detail that operates 24-hours-a-day. Within the 600-room building, 800 staff and a variety of defence and intelligence liaisons ply their trade.

Eye Spy understands the building, with an estimated value of £500 million, will not be fully vacated until about 2015.

In Eye Spy 57 and 58 we examined procedures you can take that reduce the chance of you being taken hostage. Sometimes, however, a combination of bad luck and good planning on the part of the Hostage Takers may mean that despite all reasonable precautions, you are seized. What can you expect? What actions should you take? How can you maximise your chances of a safe return home to your loved ones?

Hostage specialist **SIMON ATKINSON** presents simple measures and protocol that will maximise your chances of survival and eventual return home.

Whilst immediately applicable to military and conflict theatres, this important series also contains valuable advice for other hostage scenarios.



PART 1

RULES OF HOSTAGE SURVIVAL

by **SIMON ATKINSON**

SURVIVING CAPTIVITY



The saying that "Knowledge is Power" is crucial in Hostage Survival - a main method of control by your captors is to deny you information and allow your self-induced pressures to keep you in a state of fear.

Understanding of where you may be and what is happening to you is a vital tool in your survival toolbox.

Irrespective of the type of organisation or individual who has captured you - there are certain specific stages of captivity. It is important to be able to identify these as each stage has its own peculiarities, dangers and even opportunities that you should be aware of if you are to survive captivity.

INITIAL CAPTURE

This is a particularly dangerous stage. Of course, you may simply be killed here, you may have been stopped simply to commit roadside robbery. If there appears to be debate as to your future - try to convince them to release you - this will end the situation before it starts.

After negotiation, your next best option is escape. Escape should be attempted only if there is a good chance of success. Do not make the error in thinking that it is your duty to try to escape, even if you believe you may fail and get hurt. You should also consider the impact of your escape upon those who may be left behind. Are their chances of survival minimised if you are not there to take care of them?

If you choose violence rather than running as your escape method - then only do so if you really think you can win. If you decide to "give it a go", then there must be no half measures. Be fast, aggressive and violent. Failure at this point may mean you will be killed or viciously beaten.

If you are going to run - have a plan. Where to? It is pointless escaping a hostage scenario if you will die in the escape. However, if you can escape - then it is best to do so as early as possible. This is because you are still potentially close to friendly forces. Later stages may take you deeper into enemy territory. The noise and confusion of the attack will still be evident in the excitement of the attackers and locals - under this excitement and confusion, you might be able



German engineers Thomas Nitzschke and Rene Braeunlich appear on Al-Jazeera television less than two hours after being seized by al-Qaida terrorists in the northern industrial city of Beiji, 155 miles north of Baghdad. The strain on the men's faces is clearly evident - though they somehow kept their composure.

to slip away. Your captors at this stage may simply be soldiers and not experts in prisoner handling.

It's also the best time to escape because you have not yet been fully strip-searched and may still have items on you that may aid your subsequent evasion. Similarly, you are hopefully still fit and healthy - later on, perhaps degraded and ill, you may not have the will to escape even if the opportunity was to present itself.

Your next best option is to accept the fact that you are caught. Be compliant (passive BUT NOT submissive) - emotions will be high and you risk significant violence if you behave arrogantly or even too weak.

Expect looting of any valuables. This may be simply because your captors are poor and the sale of your wristwatch will feed their family for a month. Resistance will be met with violence. If you are not happy for it to be stolen, it should have stayed at home or on base.

Blindfolding or hooding will likely happen to maintain security of where you are going - or simply because they have seen movies where this is done and believe it to be the right thing to do. Depending on the sophistication of the hostage takers, they may be starting to "CONDITION" you - more about this later.

You will likely be roughly disarmed/searched for intelligence. This may be rank slides, ID cards, notebooks etc. Your weapons may be 'signature



Hostage-taking is not limited to war zones. This photo shows the aftermath of a hostage incident that occurred on the streets of Moscow on 26 June 2008. A man took a female hostage and claimed he was armed. City police decided not to negotiate and rammed the car freeing the captive. Each hostage incident should be carefully assessed by the security forces prior to action.

weapons' and may be of intel value. Again - did it really need to come on the ground (see Eye Spy 57 and 58 - 'Cleaning Down').

Expect rough treatment. They will want you out of the way before a security force response. Arrogance or physical resistance will be beaten from you or you may simply be killed. Your behaviours here are already being assessed and your captors are starting to reach decisions about you already.

Worst case scenario - create a plan in case they intend to conduct a roadside execution. Have a simple phrase or phrases that you can say that will convince them that you are of more value alive than dead - perhaps not quite "take me to your leader" but something that convinces them that they will be rewarded more for your capture than your execution.

After the initial furore has died down and the shooting has stopped, your mind will undergo a huge plethora of emotions. You will feel an immense relief that you are still alive, but this will rapidly be replaced by a cold fear of what may happen to you now. So many conflicting emotions prevent a coherent response and you may begin to feel like a rabbit caught in a

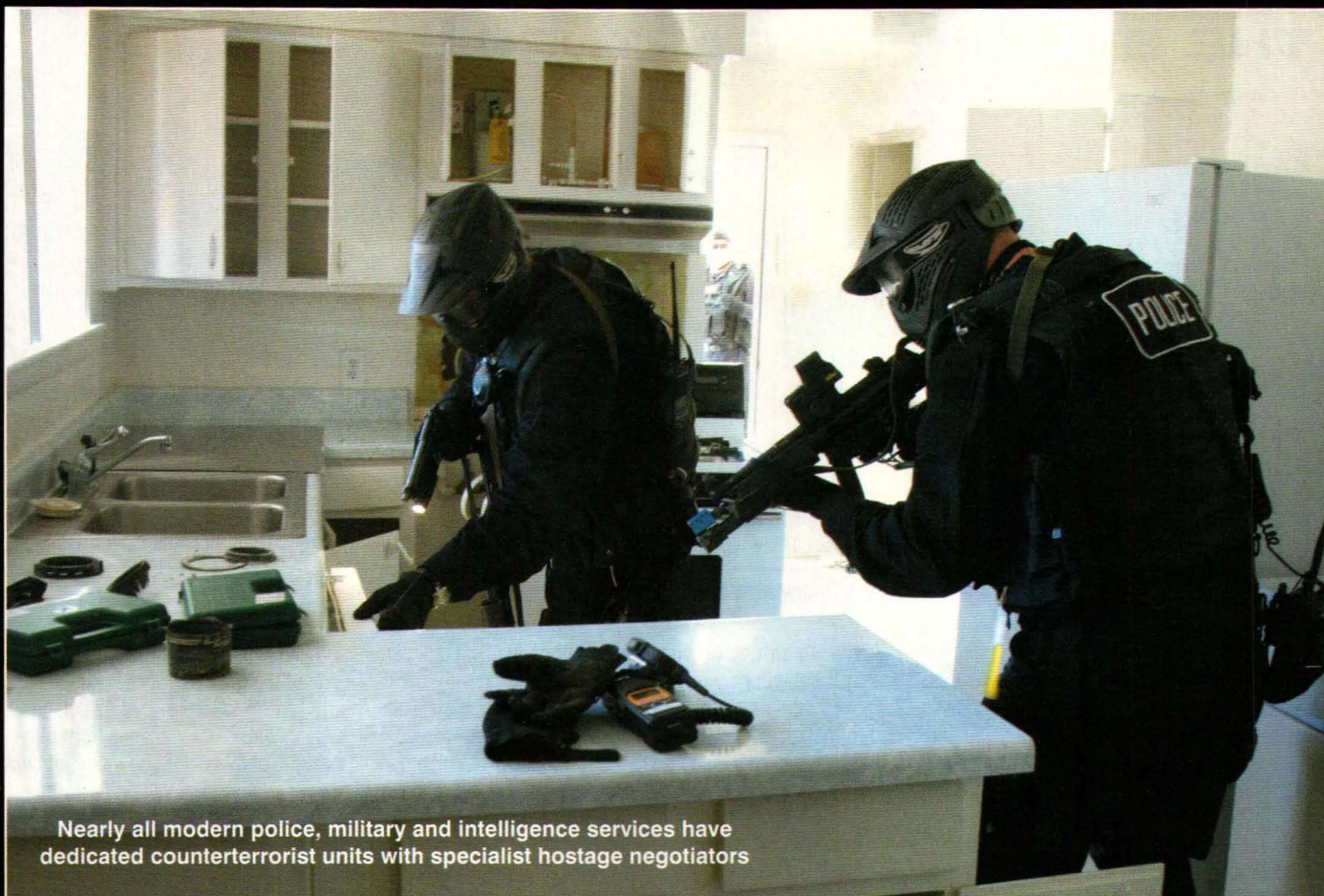
headlamp - unable to reach a decision and do anything. This mind-numbing state is known as the *Shock of Capture*.

During the period where you are under its influence, the Shock of Capture will cause you to be unquestioningly compliant and easily manipulated by the hostage takers. They will want you to stay in this condition for as long as possible and, depending upon their sophistication, they will consciously or unconsciously implement measures to prolong its effects. This is a NORMAL psychological reaction. This recognition of your state will enable you to control it, to resist panic and to make calculated and measured judgement. All hostages suffer from this but it is this knowledge that will reduce its duration.

TEMPORARY HOLDING AREA (THA)

This is the place where you will be taken immediately after capture whilst the security force reaction calms down and where the captors can continue their assessment of their "prize".

You may well find that you are exploited early, possibly by driving to the THA via a crowd who



Nearly all modern police, military and intelligence services have dedicated counterterrorist units with specialist hostage negotiators

may be angry at your government's policies in their country, for example, demonstrating the hostage takers capability to undermine your efforts. This may happen if your hostage takers have political or revenge-based aims. You will also find yourself in the unenviable position of depending upon your captors for your safety, perhaps feeling grateful towards them for protecting you! Remember - they are your enemy, they are exploiting you and they will not allow the crowd to harm you because you would then be of no further value.

At the THA, your captors may now really start their assessment of who they have caught.

Al Qaida interrogation guides infer that *"If an infidel is weak and submissive - maximise his*

potential by killing him quickly on video, in the Islamic way". If however, *"an infidel can be of further value - by video or interrogation perhaps, then take time to use him. Then kill him in the Islamic way"*.

The difference here is TIME. The longer you can stay alive, the better chance you have of being rescued or of escaping.

A criminal gang may see your value in selling you on to a terror group. In which case you may not want that to happen.

You must convince your captors of your value - alive better than dead. Be careful NOT to go too far. If your captors believe that you are "too hot to handle" they may simply kill you and leave the

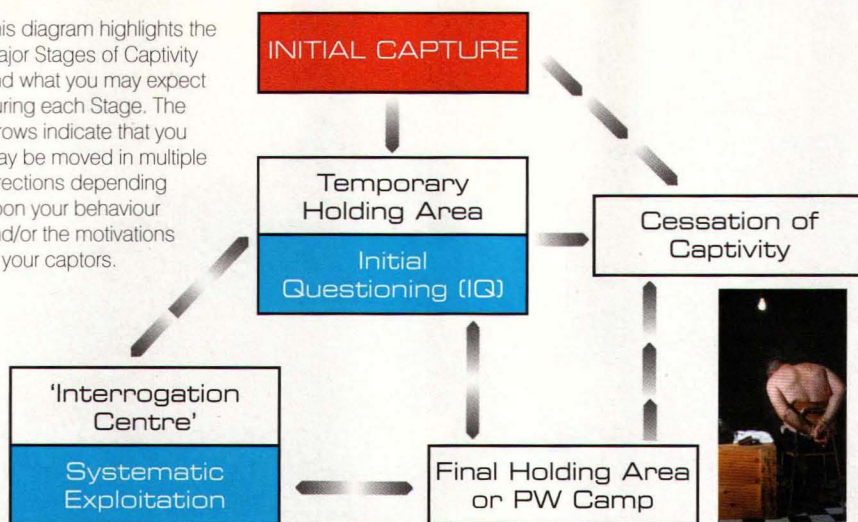
area because they will be afraid of the repercussions of capture themselves.



Black Hawk helicopters manned by counterterrorist officers prepare for a night-time exercise

THE STAGES OF CAPTURE

This diagram highlights the major Stages of Captivity and what you may expect during each Stage. The arrows indicate that you may be moved in multiple directions depending upon your behaviour and/or the motivations of your captors.



The FBI's Hostage Rescue Team (HRT) was established in 1983 to be a national level counterterrorist unit.

The next Stage of Capture is the Final Holding Area (FHA)

Your captors assess you here - but you must also assess your captors. What do they want? What do you want? Continue trying to establish rapport with individuals and humanise yourself without appearing too weak. REMEMBER - It is harder to harm a person than an object.

As you move further down the chain - your opportunities for escape are reducing. You may be moved to a number of areas depending upon the needs of your captors and the security force response to your capture.

If you are fortunate, you will miss out on the next stage, but you may have been captured by individuals motivated by the need to gain information or to systematically exploit you. You may have been passed on to a hostile intelligence agency or to a sophisticated terror cell - in which case, you may find yourself under sustained interrogation in an interrogation centre*.

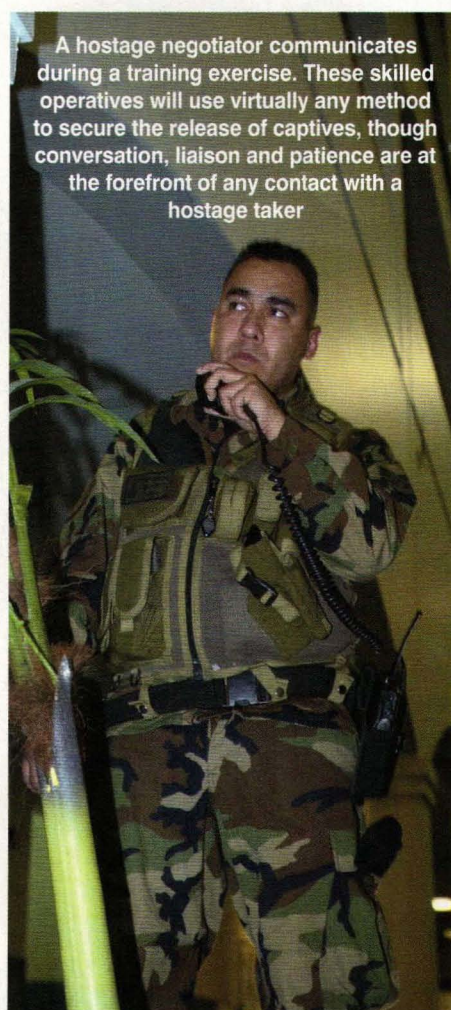
EXPLOITATION STAGE

This stage may more accurately be termed the Exploitation stage. This is where you may have been handed on to another group and questioned or exploited for their own ends. You may even have been passed along the chain within the original capturing group. You will be continually assessed so that the group can determine how best to gain from your captivity and you will be systematically exploited whilst you are still "today's news". Any holding force now will likely be experienced and you will have little or any opportunity to escape at this stage. However, you may be returned to this stage as your captivity progresses and be further exploited in order to keep the pressure on your organisation or government.

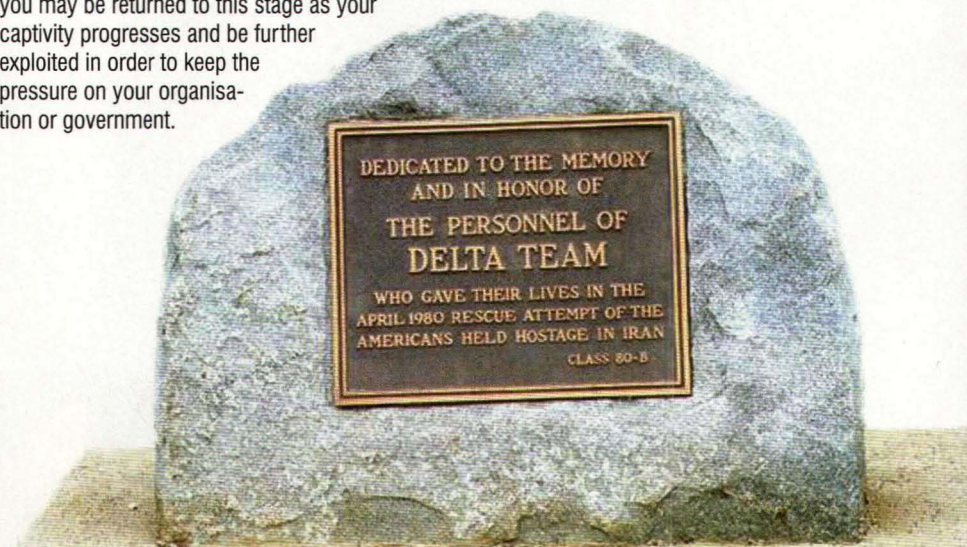
This is where you may be taken to complete your incarceration and is likely to be far from the Forward Edge of the Battle Area - i.e. - deep inside enemy controlled territory. At this stage you may be held with other hostages from other organisations. It's at this point you must get back to planning your escape. You will probably be held here for a certain amount of time which allows you an opportunity to determine routines and assess other information required to plan an escape.

Third party organisations may still be interested in you - you may be visited at some times by other criminals/terrorists or indeed members of international organisations. Negotiations will be continuing even though you may not hear news. (We will explore the NEGOTIATION PROCESS in issue 62.)

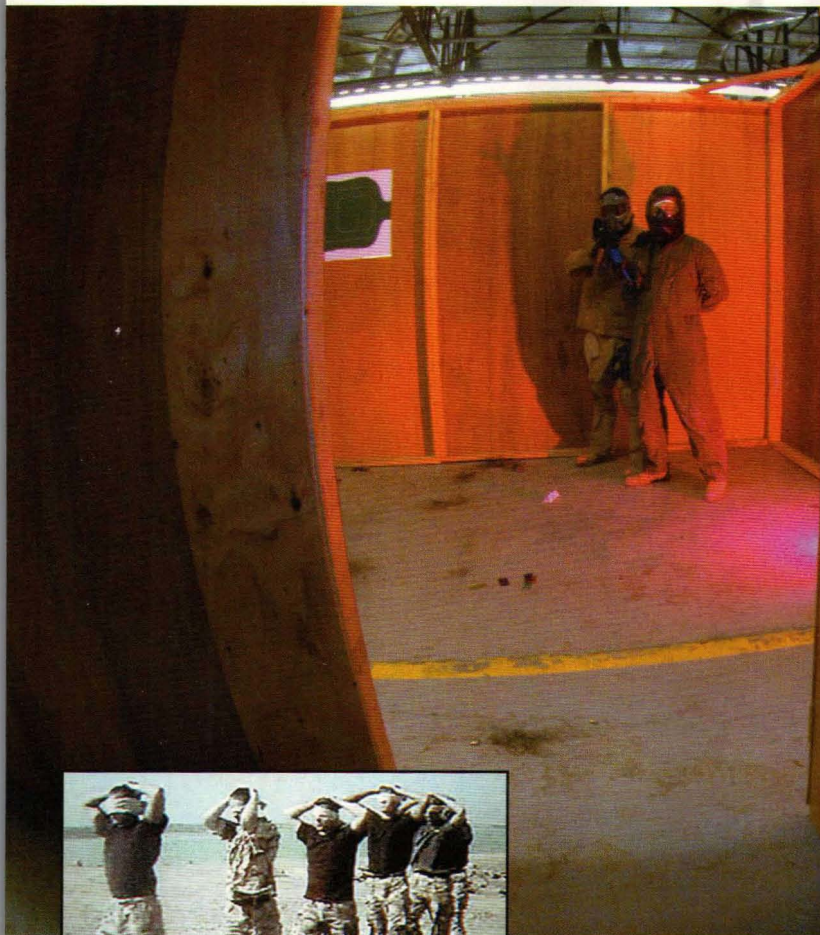
Deadlines come and go. These are particularly dangerous times and emotions run high in expectation of a course of action that may not come. Perhaps you will be told you are being released, but be careful not to build up your



A hostage negotiator communicates during a training exercise. These skilled operatives will use virtually any method to secure the release of captives, though conversation, liaison and patience are at the forefront of any contact with a hostage taker



Any rescue attempt is dangerous - even those performed by professionals. This is evidenced by the plaque in honour of Delta Team members who died in the daring operation to release American hostages seized by Iran at the US Embassy in 1980.



US troops specialised in counterterrorist activities, engage in a hostage rescue simulation operation



British troops blindfolded and weaponless are taken hostage by Iranian forces in 2004. A similar incident occurred three years later, also involving UK maritime forces. On both occasions government intervention ensured the release of the troops - who were never in danger - but Iran had made its point.

expectations as the release may not happen - a cruel joke or perhaps negotiations simply stalled. "False release" can be particularly draining as you will be bitterly upset and disappointed. Do not expect release until you are in the hands of your employers or an international organisation such as the Red Cross/Red Crescent or something similar.

CESSATION OF CAPTIVITY

There are a number of circumstances that will result in the end of your captivity. You could be released - signs of which may be a change for the better in the guard mindset. Your food might improve and any beatings cease. Perhaps new clothes and healthcare are afforded. This is all to ensure you appear as if your captivity was relatively benevolent. If any comforts such as these are offered, take them. Be aware of feelings of guilt amongst those released early, leaving colleagues still in captivity - this is a normal emotion. Your release may come without warning - possibly as a result of ongoing negotiations which you have not been aware of.

Escape: You escape from captivity.

Rescue: You are rescued. This is arguably the most dangerous time and every bit as dangerous as your initial capture. Think ahead and plan your actions if you suspect a rescue is underway.

Your rescuers may be local security forces with little or no knowledge or experience of counterterrorist situations. Their language skills may mean they cannot communicate directly with you and their training levels are in doubt. It's possible they do not know exactly where you are or what you even look like.

Rescue is likely to be fast and noisy. Prepare in advance - look for places you can lie low away from doors and windows. Get onto the ground and ensure your hands are visible. Do not do anything that may cause them to think you are a terrorist. You will likely be treated roughly by your rescuers until they can identify you as a hostage and not a hostage taker - you should not object to this but simply go with the flow and do exactly as you are told at all times. The last thing you want at this stage is to be regarded as a terrorist by accident and possibly killed.



Many firms who operate in uncertain areas now educate employees about hostage survival

Though studying preventive measures in order to lessen the chance of being taken hostage is essential - it is inevitable that there will always be victims



You will be better mentally prepared to deal with your situation if you understand and recognise the "Stages of Capture". The "Shock of Capture effect" will be reduced and you will be better placed to deal with other psychological pressures.

A WILL TO SURVIVE

This is a critical part of hostage survival. Many survival instructors agree that it is the will to survive that is the most important thing to develop in any survival situation. Psychological pressures experienced by the unaware or untrained hostage will erode that will over time. It is vital captives realise they are not superhuman - that they will feel and experience a complex list of emotions. Understanding this is entirely normal and expected - is key to survival. The next step is for the captive to learn how to manipulate their circumstances in order to remove or minimise such pressures.

Failure to appreciate these pressures, and take positive steps to alleviate them, often leads to a spiral of despair, depression and sometimes even suicide or suicide by proxy. When under unaccustomed stress, your actions and behaviour will revert to a basic state. This can create many difficulties in a hostage situation, particularly if that natural state is an extreme

of aggression or submission. Stress is, in itself, to be expected given the extreme circumstance of the hostage. It is the ability to recognise signs of stress - and then to make attempts to control them - that are crucial.

Standard indicators of stress build up (awareness of) are:

NARROWED COGNITION: When we become stressed we essentially regress from greater to lesser levels of expertise. Our ability to "see the entire picture" diminishes and we focus on one or two seemingly major issues to the cost of everything else around us.

IRRITABILITY: Higher stress levels inhibit our ability to concentrate effectively as well as cause us to become "jumpy" and overreact to situations which we would otherwise cope with in a different manner.

PSYCHOMOTOR DEGRADATION: Put simply - we start to shake! Our ability to conduct



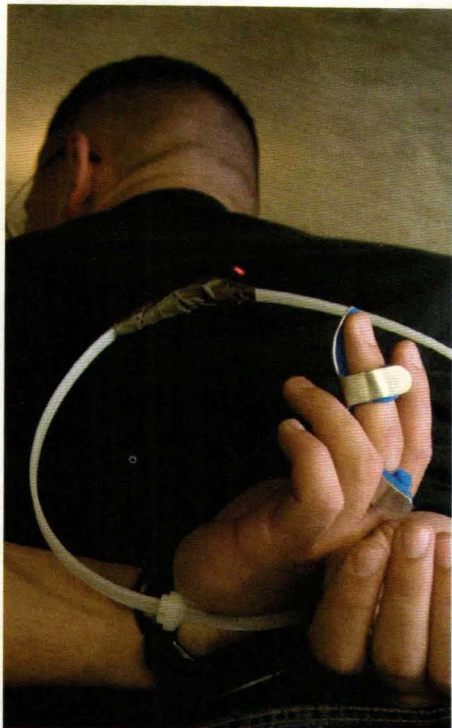
Specialists analyse a map to determine the best points where to deploy observers. If a captive can stay alive - the chances of rescue and survival improve

otherwise simple tasks becomes impaired as our levels of concentration decrease.

These physical reactions are sometimes known as **SYMPATHETIC SWING**. When in a long term stressful situation, the body adapts to that demand level and may lead to a reduction to cope with further stress and minor infections, leading to breakdown and illness.

Your aim, as a Hostage, is to create a **PARASYMPATHETIC SWING** by using coping mechanisms described later to reduce the level of stress.

There are recognisable phases of stress during and post-captivity. Recognising these in yourself and others may help you to reassert control and reduce the risk of unnecessary harm.



PHASES OF STRESS

SHOCK AND DENIAL: "Shock of Capture" is a term meaning just that. It is a physical and wholly expected state that the hostage will enter into in the moments immediately following capture. During this time, hostages are like the stereotypical "deer in a headlamp" and are extremely malleable and compliant. Hostage takers will often seek to maintain this condition for as long as possible by imposing a series of pressures on a captive. Victims will feel numb and often just simply do not believe what has happened to them.

REALITY: Described as a "terror induced pseudo calm". Victims begin to realise what has just happened and that it is real. The gravity of the situation begins to sink in.

ADAPTATION: The body adapts to stressful conditions. With hostages, this adaptation

seems to occur on a scale from total identification and sympathy to total rejection of the hostage takers and their aims by reinforcing his own identity. He maintains he is the victim of a crime.

DEPRESSION: A victim may feel abandoned with no hope of rescue or release. This may occasionally be lifted with the occasional promise of release, but this then leads to severe psychological troughs if those hopes are not realised.

RESOLUTION AND REHABILITATION: The experience is so traumatic (in psychological terms a "Primary Experience") the victim registers much of it on an unconscious level. This may lead to flashbacks/nightmares during and post-captivity. Individuals deal with this differently. All hostages seem to be helped by the opportunity to, as early as possible, discuss their experience with others who have had similar experiences. In the case of a solo experience or kidnap it is more difficult because he or she may feel that nobody can understand what they have endured. Most successful methods of dealing with this are to get groups of victims to meet and openly discuss their feelings/emotions.

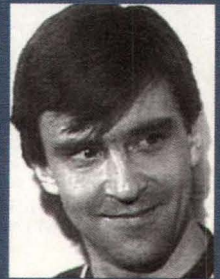
Short term after effects of intense stress are:

- Anxiety: Fear of the dark, footsteps....
- Nightmares Fear of recapture
- Instability. Fits of crying
- Criticism of police and government policy
- Sexual impotence and anorexia

Medium/longer term after effects to expect may be:

THE FIVE-YEAR HOSTAGE

Journalist John McCarthy, kidnapped by the terrorist group Islamic Jihad in April 1986, survived five years in captivity, making him Britain's longest-held hostage. The terror group, recognising his impartial reporting, and the fact that he was a "valuable Western hostage", eventually released him with a "letter" which was intended for personal delivery to the UN Secretary General.



- Concentration/memory problems
- Reduced interest in work
- Light depression
- Oversensitivity
- Bitterness and reproach toward others
- Recognition for suffering endured
- Feelings of desertion
- Interpersonal relationship problems
- Lack of interest in less important issues

* Interrogation is defined as the 'Systematic extraction of information, from selected individuals in order to obtain accurate and timely intelligence'. Resistance to Interrogation will be explored in later articles.

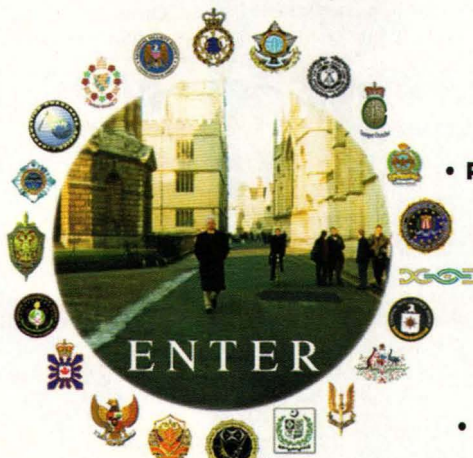
In the next issue, Simon explores a variety of psychological and physical coping mechanisms that you can use to assist you in surviving captivity.

EYE SPY

INTELLIGENCE MAGAZINE

www.eyespymag.com

24 HOURS A DAY



Welcome to **Eye Spy** Magazine

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



READERS PLEASE NOTE: All prices include VAT (UK) and shipping!



ESPL ON-LINE

TEL. 01756 770199 UK / TOLL FREE 877 309 9243 USA

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 concerns you.

GSM BUGS

Eye Spy provides an interesting range of custom built GSM bugs (Global System for Mobile Communications). Unlike UHF transmitters, these fully functioning everyday devices contain a concealed SIM card allowing you to call them from anywhere in the world and listen-in via two powerful microphones.

This fully functioning GSM wall plug adapter comprises of the very best components and materials for superior listening quality. When called, the unit does not ring, vibrate or reveal the device has opened-up a twin-microphone listening channel. Ideal for office or room environment. Mains powered for continuous surveillance.

Also available in the GSB bug range: Mini economy bug, wall socket, picture frame, extension lead, clock, calculator, lamp shade, umbrella and smoke detector



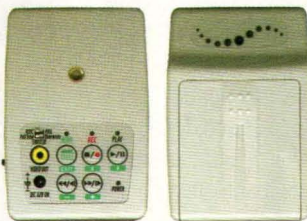
NOW HALF PRICE!
£225.00 OFF!
GSM Plug Adapter Bug:
Order code: ES-GSM1 UK £225.00
USUAL PRICE £450.00

TELEPHONE TAP DEFEATER and Room Bug Hunter

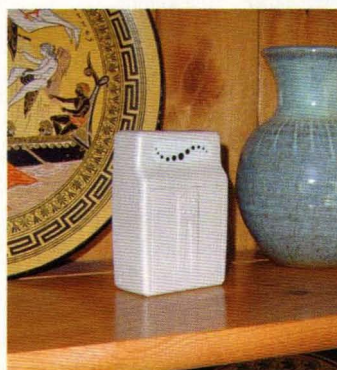
Locates virtually any type of transmitter to the high frequency coverage area. LED display, comes with crocodile attachment check for telephone bugs within 5 metres the connection point. Uses PP3 battery
UK £195.00 USA \$350 ROW: £220.00
Order code: LS-RFTT

HOMEGUARD 2

Personal security digital video recorder. Homeguard is a simple but utterly dependable home or office security surveillance system that requires no wiring, software or exterior power source. Simply place where you require video footage. It will record continuously or take snap shots at given intervals. Now with audio. Looks just like an air freshener/purifier.



UK £249.00 USA \$325.00
ROW: £260.00
Order code: TX-HOMEGUARD



SOUNDPOD

Super amplified 'SoundPod' broadcast quality sound amplification in an ipod size. Ultra sensitive directional microphone picks up sound upto 100 feet away. Volume, treble and bass control. Broadcast quality can be used indoors or out. Low cost useful device.

Order code:
TX-SPR
UK £40.00
USA \$60.00
ROW £40.00



EYE SPY SEED MICROPHONE

Seed microphone so small it can be concealed anywhere - hide in a car, under door, bag, sleeve, belt etc. The length of lead is 36 inches - but we can customise this for you - £1.00 (\$1.75) for every additional 12 inches. The microphone head is just 5mm wide.

Order Code: LS-SM1 UK £17.50 USA \$38.00 ROW £18.00

EYE SPY PEN MICROPHONE



Contained inside the ordinary pen is a powerful microphone. Simply plug the lead into a recorder and record any conversation without the worry of trying to hide a body-worn microphone. Can be hidden in a desk etc.

Order code: L-PN1 UK £25.00
USA \$48.00 ROW £28.00

MINI MIC

Eye Spy's Mini Mic is designed for all microphone uses. Excellent quality at a low price for voice recording - superb sound pick-up. 15ft. cable - on/off switch.



Order code: ESMU UK £30.00
USA \$48.00 ROW £35.00

FINGERPRINT READER

SECURE DIGITAL STORAGE

This Fingerprint Reader features a built-in Sweep-type Fingerprint sensor to secure your data, 1 gigabyte storage capacity and a USB 2.0 interface for quick data transfers.

Application features include web auto login to manage the entries of ID and password for the web sites you visit, user settings for fingerprint registration, password settings and fingerprint live time setting, file and folder settings to encrypt or decrypt files and folders and PC lock to prevent others from using your computer while you're away. Just plug in the drive, swipe your finger, and you can log on to any of your stored protected areas in an instant. For more details and full specifications visit www.eyespyimg.com



Order code: FR/D UK £69.99
USA \$120.00 ROW £75.00

SOUND PRO II HIGH PERFORMANCE SHOTGUN MIC

Super amplified shotgun microphone with fantastic sound enhancement and noise cancelling, recording jack, camera mount and superior Sony earphones. All cables included. Quality product comes in hard-plastic carry case.



SPY FINDER



WORLD'S MOST POPULAR COVERT CAMERA DETECTOR

Reliable and easy to use technology. Ideal for defeating hotel and office snoopers. Simply scan the room and hidden cameras return the beam which resembles a flashing pulsating light.

Order code: ES/SFI
UK £68.00 USA \$119.00
ROW £95.00



UK £200.00 USA \$320.00
ROW: £230.00
Order code: TX-SP2SM

OUTDOOR STEALTH CAM

OUTDOOR STEALTHCAM DIGITAL VIDEO INFRARED VIDEO RECORDER

High quality VGA day or night adjustable takes 50 to 90 second clips. Time, date, moon phase, and temperature stamp. 5.0 mega pixel day colour shots and 2.0 night black and white. Burst mode allows 1 to 9 pictures per second, no flash 42 emitter infrared emitters illuminates 50 feet. 32 MB built-in internal memory with expandable memory using up to 2MB SD card.



Order code: TX-SE UK £325.00
USA \$525.00 ROW £335.00

ELECTRONIC RADAR WATCHDOG



This highly rated product is one of the best anti-burglar-intruder systems available today. Simply turn on (no installation required) and the realistic dog bark sound increases as its internal radar senses someone approaching the door. Bark gets louder as person nears door. Going on holiday or just going out? Protect your home, family or office with this superb security system.



Order code: TX-EWREX UK £90.00 USA \$125.00 ROW: £100.00

VIDEOTEK & MINI

LOCATES AND VIEWS ANY SECRET TRANSMITTING CAMERA

The world's most popular wireless camera hunter now comes in two sizes. VideoTek and VideoTek Mini locks-on to any wireless video camera and displays the transmission on its built-in screen. Automatically scans all the commonly used video frequencies in less than five seconds and locks-in on any video camera transmitter. Besides displaying what the covert camera sees, it also sounds an audible alert tone. Selectable antenna sensitivity allows lock-in on sources up to 500ft away (depending on power of source transmitter). Durable all-metal case. Eye Spy recommended for countermeasures.



**NEW
LOWER
PRICE!**

Standard: Order code: TX-VIDTEK
UK £350.00 USA \$485.00 ROW: £370.00

Mini: Order code: TX-VIDTEKMINI
UK £375.00 USA \$525.00 ROW: £400.00



AJ-34 AUDIO JAMMER

RECORDING COUNTERMEASURES

The AJ-34 Audio Jammer protects your sensitive room conversations by generating a random masking sound which desensitizes any nearby microphone. Effective against any microphone-based eavesdropping device including tape recorders, RF transmitters, hard-wired microphones (including contact type) and shotgun microphones. It also protects against microwave or laser reflection pickups. Covers 150 square foot area.

An effective device that can be likened to "white noise" - works very well in most environments.

Order code: AJ-34 UK £90.00 USA \$140.00 ROW £100.00



COVERT BLACK

ECONOMY

HIGH-QUALITY COVERT CAMERA AND AUDIO RECORDER PLUS COLOUR DISPLAY



SPECIAL SUBSCRIBER
PRICE UK £325.00

USA \$599.00 ROW £375

Order Code: CBE-LESUB

**SUBSCRIBERS
SAVE £50.00
\$100.00!**

Capture video and audio easily and safely without fear of compromise. View film on display, computer or television. All leads supplied for a variety of tasks. Powered internally (no leads or exterior battery). Set comes in a smart polished metal and black case.

SET INCLUDES

High-quality button camera with matching set of buttons; built-in sensitive microphone; NTSC/PAL compatible display - 380 TV lines; multi-function recorder MP4 player; supports multi-language display; transfer tools included; 6-8 hours of recording time. Quality earphones supplied for discreet listening.



UK £375.00 USA \$699.00 ROW £400.00 Order Code: CBE-LE

ENIGMA COMINT

**EYE SPY'S FIRST EVER
FULLY FUNCTIONING
SPY CELL PHONE**

Order code: ENIGMA-COMINT: UK £295 USA \$590.00 ROW £310.00

Dial the number and the cell phone will not ring, light-up or vibrate. The microphone, however, will open allowing you to listen to surrounding conversations wherever the phone is placed (worldwide). Unlike our Enigma's, the COMINT cell phone is a working unit!

EYE SPY SMOKE DETECTOR UHF TRANSMITTER

**SAVE 50%
(£100.00 •
\$200.00)**



High-quality fully-functioning smoke detector that incorporates UHF transmitter. Built by Eye Spy the unit will continue to transmit even if alarm sounds or is tested. Removing back of smoke detector to replace battery will not reveal bug. The unit also comes in original packing therefore defusing any suspicion over its covert function. Range 500ft.

Order code: ES-SDUHF

UK was £199.00 **NOW £99.00**
USA was \$399.00 **NOW \$200.00**
ROW was \$210.00 **NOW £105.00**

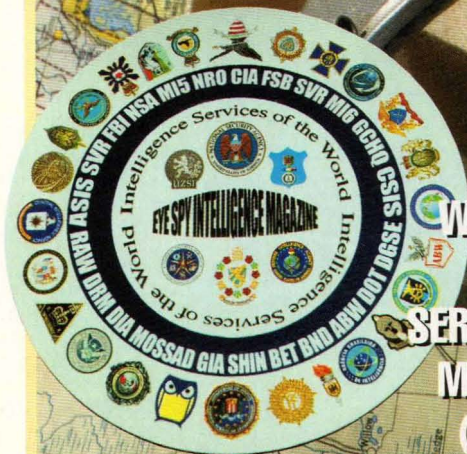
EYE SPY

INTELLIGENCE MAGAZINE

SUBSCRIBE

FREE

WITH EVERY SUBSCRIPTION
EYE SPY'S INTELLIGENCE
SERVICES OF THE WORLD MOUSE
MAT WORTH £7.99 (\$17.00)
(NEW SUBSCRIBERS ONLY)



UNITED KINGDOM, USA, EUROPE, ROW

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

UK 1 YEAR £27.50 ☐ USA 1 YEAR \$49.99 ☐ EUROPE/ROW 1 YEAR £30.00 ☐

UK 2 YEAR £50.00 ☐ USA 2 YEAR \$96.00 ☐ EUROPE/ROW 2 YEAR £55.00 ☐

A subscription will protect you against any price increase

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, American Express, Switch (UK)

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@eyespyimag.com **ONLINE** www.eyespyimag.com



UK, EUROPE, ROW

Send your subscription to:

Eye Spy Publishing Ltd

P O Box 10, Skipton,

Leeds City Region, 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
12.00pm - 6.00pm, Mon-Fri



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

ESPI_2009_OD/PS/I/616161

COMPL

EYE SPY IN

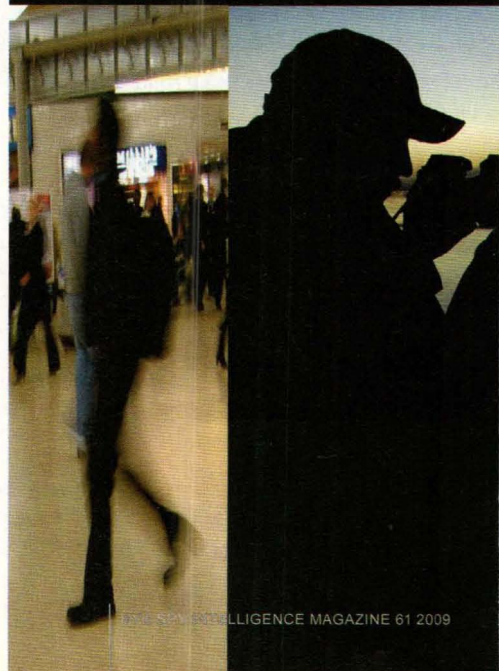
VOLUME 2 COMPLETE

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

OUTST

ALL VOLUMES COME WITH
A FREE EYE SPY BINDER

PRICE INCLUDES
P & P AND AIR MAIL COST
TO ALL COUNTRIES!



TE VOLUMES

LLIGENCE MAGAZINE

VOLUME 3 COMPLETE

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

VOLUME 4 COMPLETE

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

NDING VALUE

VOLUME 5 COMPLETE

Volume V
Ref: ESVOL5
UK £32.50
USA \$55.00
ROW £37.50

VOLUME 6 COMPLETE

Volume VI
Ref: ESVOL6
UK £35.00
USA \$60.00
ROW £40.00

VOLUME 7 COMPLETE

Volume VII
Ref: ESVOL7
UK £35.00
USA \$60.00
ROW £40.00

COMPLETE YOUR EYE SPY COLLECTION

Volume Two (eight issues)
numbers 9-16

Volume Three (eight issues)
numbers 17-24

Volume Four (eight issues)
numbers 25-32

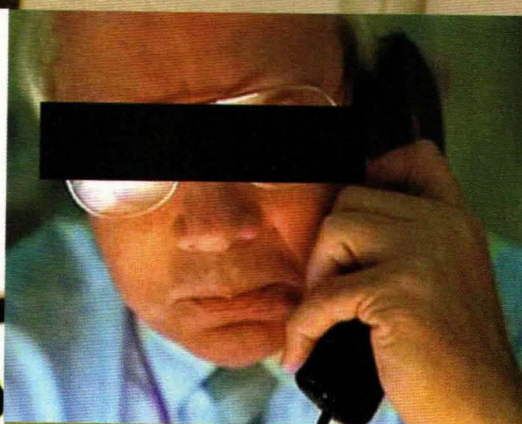
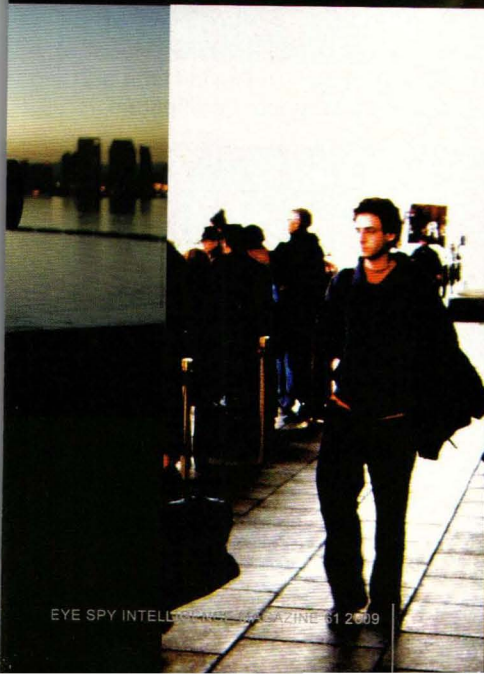
Volume Five (eight issues)
numbers 33-40

Issue 36 out of print. Magazine included on a CD in PDF format.

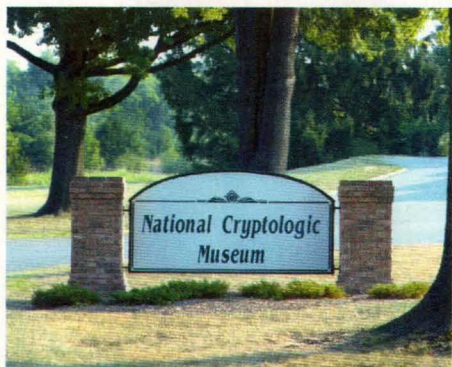
Volume Six (eight issues)
numbers 41-48

Volume Seven (eight issues)
numbers 49-56

OBTAIN THE SECOND,
THIRD, FOURTH, FIFTH,
SIXTH AND SEVENTH
YEARS' ENTIRE
COLLECTION OF THE
WORLD'S LEADING AND
MOST POPULAR
INTELLIGENCE
MAGAZINE...
EYE SPY



Letter from Fort Meade by David Hamer



The National Cryptologic Museum Foundation (NCMF) recently presented a symposium to commemorate the 1941 attack on Pearl Harbor by Japanese naval forces.

The occasion was preceded and highlighted by two events: the gala opening of an expanded museum exhibit of Japanese and American cryptographic material and the announcement of a new CCH publication, *'West Wind Clear - Cryptology and the Winds Message Controversy - A Documentary History'* by CCH historians Robert J. Hanyok and the late David P. Mowry.

THE NEW EXHIBIT

American codebreakers of the WWII era assigned 'colourful' codenames to the various targets of their concerted attacks. The newly opened exhibit contains, in chronological order, examples of the RED, PURPLE and JADE machines...

RED: In the 1930s Japan attempted to buy an advanced cipher machine from Boris Hagelin's newly-formed company in Sweden but Hagelin, suspecting that the Japanese were purchasing it only to duplicate it, supplied them with examples of an obsolescent design patented by his former business partner, Arvid Damm. Hagelin was justified in these suspicions: the Japanese did indeed 'reverse engineer' the Damm machine and put

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

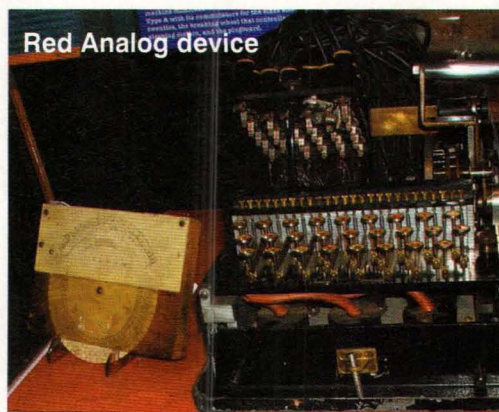
WEST WIND & PEARL HARBOR



Dr David Hatch, Mr Robert Hanyok, Mr Stephen Budiansky, Dr David Kahn and Dr John Ferris discuss Pearl Harbor and associated Signals intelligence

examples of the reconstituted machine into use by both naval and diplomatic sources. The Japanese named this machine angoo-ki-tai-pu A - Cipher Machine Type 'A'

The 'RED' component of the new exhibit contains a newly-discovered blueprint of the machine as drawn 'post facto' by US Navy engineers that carries a handwritten note by famed American cryptologist Frank B. Rowlett: "I doubt this is an original RED machine drawing... I believe the drawing was prepared by the US Navy Model Shop..." [The note is signed by Frank Rowlett and dated 17 August



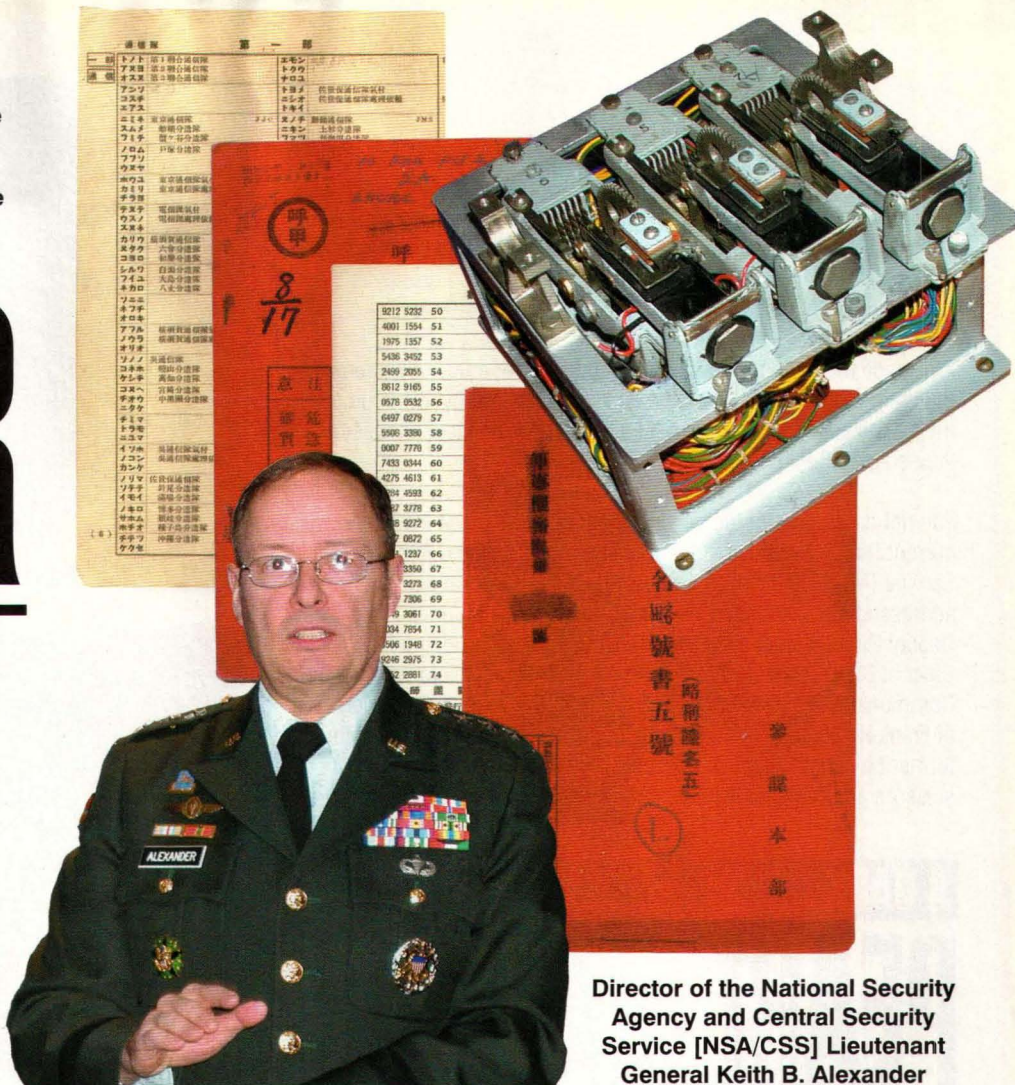
Right: **PURPLE**: The largest of three surviving pieces of the famous Japanese diplomatic cipher machine recovered from the wreckage of the Japanese Embassy in Berlin, 1945. Other Japanese code books are also pictured

CLEAR SYMPOSIUM

1975]. Alongside is an example of a hand-operated RED analog device together with an automated RED analog machine, built in the late 1930s by the Navy Yard Model Shop in co-operation with the US Army's Signals Intelligence Service. The machine mimicked and duplicated the actions of Cipher machine Type 'A'.

JADE: The US codebreakers' name for the high-level encryption system used by the Japanese Navy. Cryptanalysis of JADE was made more difficult by the fact that its messages used the forty-eight character katakana syllabary. The particular example of the JADE machine in the NCM display was captured during the US attack on the island of Saipan in June 1944. JADE was known to the Japanese as 97-shiki inji-ki-1 2.

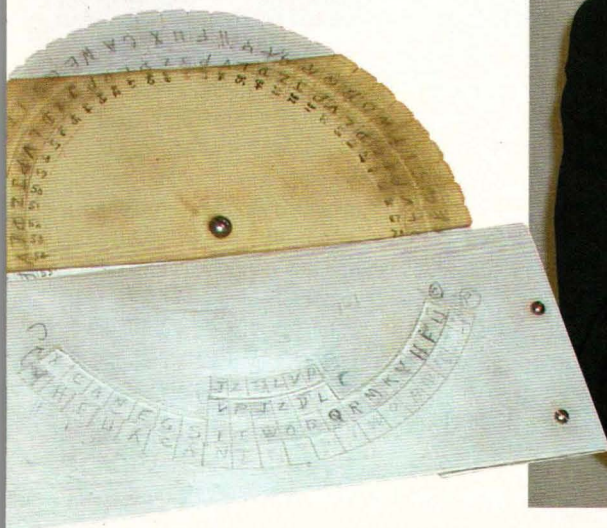
PURPLE: Two examples of the US-built analog for attacking this machine, designated angoo-ki-tai-pu B or Cipher Machine Type B, are in the



Director of the National Security Agency and Central Security Service [NSA/CSS] Lieutenant General Keith B. Alexander



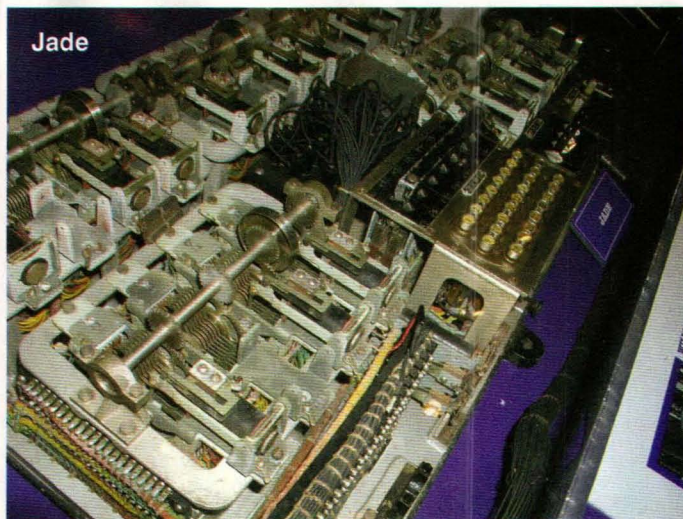
Curator of the NSA's Cryptologic museum Mr Patrick Weadon addresses symposium delegates



new display: the first was constructed in 1940 and has a decidedly 'breadboard' appearance. During a post-war visit to NSA Frank Rowlett identified this device as being the actual device used to decrypt the critical message that revealed Japan's intention to break diplomatic ties with the USA in 1941: the second PURPLE analog on display is a much improved, and consequently larger, version built in 1944.

Alongside this group of SIGINT artefacts sits the only known remaining fragment of an actual PURPLE machine, recovered by allied forces from the basement remains of the destroyed Japanese Embassy when they entered Berlin.

The ribbon-cutting for the newly enhanced exhibit was led by the current Director of the National Security Agency and Central Security Service [NSA/CSS] Lieutenant General Keith B. Alexander who addressed the assembled visitors and dignitaries before inviting the Deputy Director, John C. (Chris) Inglis; Deborah A. Bonanni, NSA's Chief of Staff; Judith A. Emmel, NSA's Associate Director of Strategic Communications; Gene Becker, President of NCMF; Tom Rowlett, son of Frank Rowlett, designer and builder of the original Purple analog; and former Museum Curator, Jack E. Ingram, to pick up their golden scissors and participate in the cutting of the ceremonial ribbon.



© DAVID HAMER



© JOHN GARCIA

A DARK CONSPIRACY AT SPECIAL REPORT

PEARL HARBOR?

Panel Discussion on Pearl Harbor and Associated Signals Intelligence

As with most, perhaps all, events that are literally earth shaking - examples are the sinking of the Battleship Maine, the attack on Pearl Harbor and, more recently, the 9/11 attack on the World Trade Center - even before the dust has settled the conspiracy theorists began their work.

The premise behind the Pearl Harbor attack as proposed by those theorists is that President Franklin Delano Roosevelt (FDR) provoked the attack on Hawaii, knew about it in advance and covered up his failure to warn his military commanders and members of the United States government. The theorists were, and still are, convinced that FDR needed the Japanese attack as a reason to force Germany

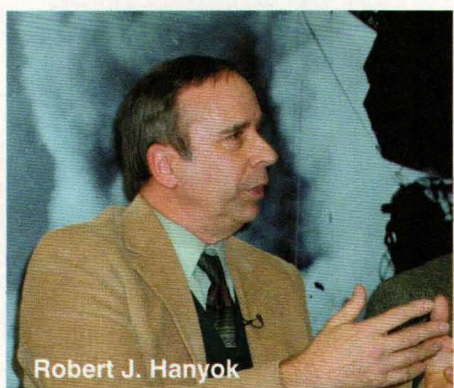


into a declaration of war, since the American public and US Congress were overwhelmingly against becoming involved in the European conflict. It has been described as "FDR's backdoor to war".

At the opening of an exhibit at the National Cryptologic Museum a six-member group of military historians convened to discuss the book, *West Wind Clear*, by Robert J. Hanyok and the late David P. Mowry, published by NSA's Center for Cryptologic History.* This volume, drawn from official and other reliable sources, considers all of the historical aspects of the attack without the usual "conspiracy"

overtones. The panel found no evidence to support theoretic inferences and allegations that FDR, together with Winston Churchill, manipulated the Pearl Harbor attack for his own political purposes. The panel and the participating audience, many of whom were former government SIGINT and COMSEC specialists, arrived at a consensus that the events of 7 November 1941 carried no overtones of conspiracy, though a number of operational errors made by the US authorities contributed to the severity of the ensuing operational chaos.

* The event was organised by NSA's Center for Cryptologic History [CCH] and supported by NCMF



Robert J. Hanyok

'GEMS' IN THE NSA CLOSET

Discovery of the 'Holy Grail'

In the course of updating the inventory records at the National Cryptologic Museum (NCM) a number of noteworthy items have come to light. Two will be of particular interest to students and collectors of cipher machines... others will be presented in future issues of Eye Spy

Enigma

At this point in time it is probably not an earth-shaking news event to have recovered yet another Enigma machine, but Enigma A766 is believed to be among one of the oldest of the commercial machines to be extant. This Enigma's principle claim to fame, a passive one, is that it was one of two Enigmas to be purchased by the United States government, for purposes of evaluation - the other being A772 - circa January 1928.

There were no surprises when a team consisting of Enigma specialists including James Oram and myself carefully measured the internal wiring of this machine and found it to be of standard configuration, based upon already-published data for the Commercial Enigma K. Other than minor cosmetic details A766 is identical to a number of other, later Enigmas of this type that we have examined

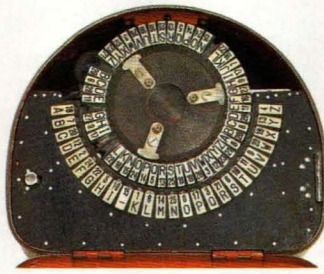
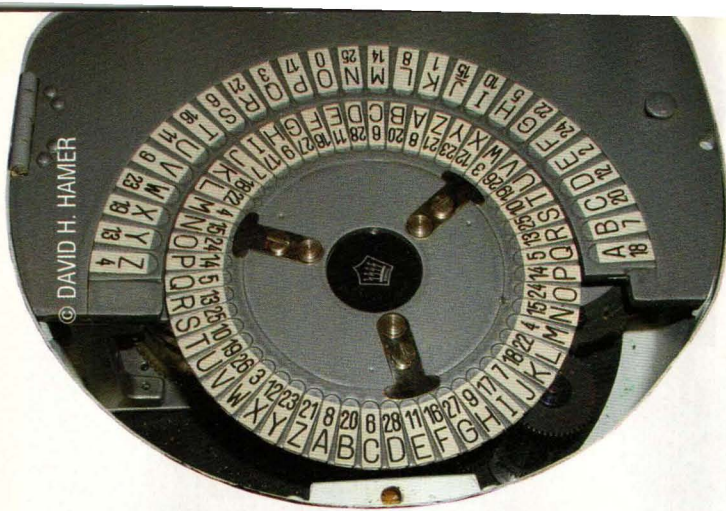
over the years. Early Commercial Enigma K machines were given 'A' prefixes to their production serial numbers... at some later point this system of numbering was replaced by the more logical 'K' prefix but the wiring and other details of the Commercial K machine remained unchanged. A766 was at some point modified, probably by the US evaluation team, to run from an external power supply. This Enigma is in fairly good condition given its age and seems to function well mechanically, though it has a large crack in the oak outer case and the latch to the case is missing.

As one Enigma researcher said when being told about A766... "To an Enigma aficionado this discovery is akin to finding the Holy Grail..."

Kryha

The inventory has revealed information about other cipher devices at NCM - one of which is the Kryha machine. Alexander von Kryha applied for the appropriate patents in both Germany and the USA in 1924 and 1925 respectively. A US

© JAMES W. ORAM



COURTESY JERRY PROC

patent - #1,744,347 - was granted in January 1930.

According to an encyclopedia entry: "The Kryha machine was a device for encryption and decryption, appearing in the early 1920s and used until the 1950s. The machine was the invention of Alexander von Kryha, a Ukrainian engineer based in Berlin. There were several versions; the standard Kryha machine weighed around five kilograms...."

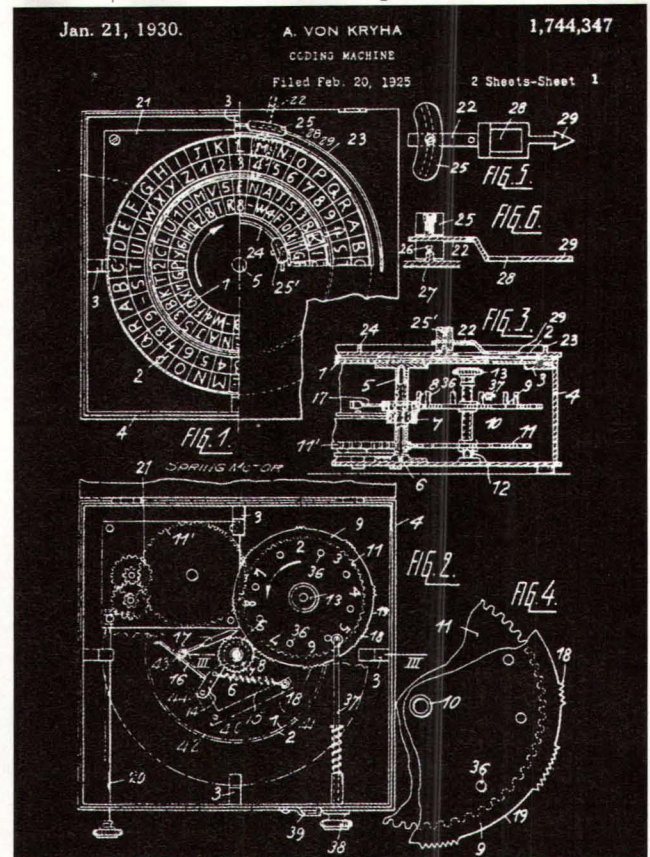
Kryha was used initially by the German diplomatic corps and later by Abwehr - the intelligence arm of the German military. Like the Commercial Enigma Kryha was

evaluated by US military. Intelligence cipher experts William Friedman and his aides Solomon Kullback, Frank Rowlett and Abraham Sinkov 'cracked' rather atypically long message enciphered on the Kryha machine in a little under three hours. Kryha was not adopted by the USA for military use but did see service with "...most of the central European powers and Japan."

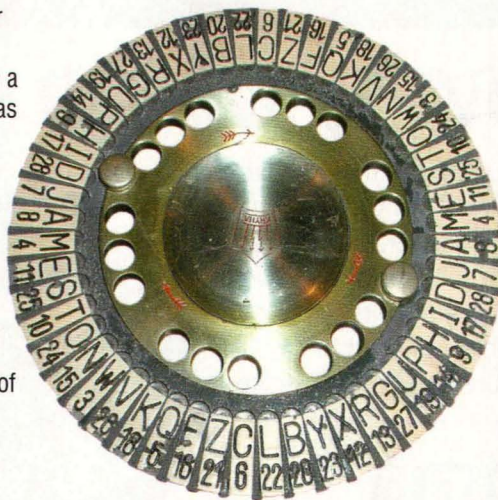
The majority of the images included here were taken in the course of an evaluation of a standard mechanical evaluation of Kryha.

© 2009 DAVID HAMER

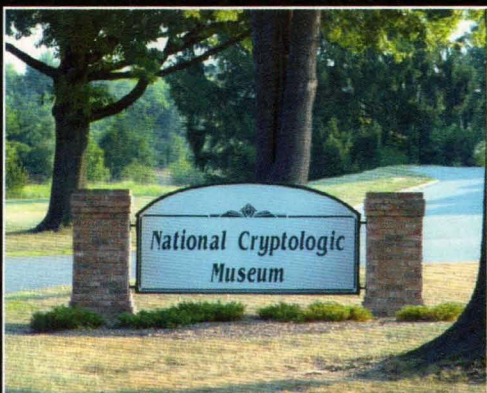
The actual patent - #1,744,347 - was granted on 21 January 1930



© CRYPTOLOGIA



For a great family day out visit America's most fascinating intelligence museum
the NSA's National Cryptologic Museum
 SUPERB AUTHENTIC DISPLAYS

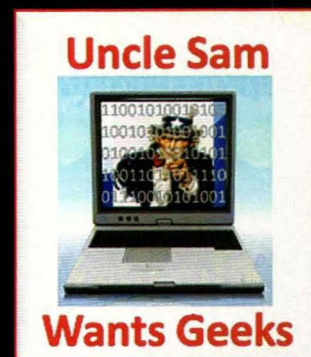


"...An entralling journey and insight into the world of the real codemakers and code breakers.. the people, machines and clandestine operations!"



www.nsa.gov/MUSEUM/

Each and every day, each and every hour, cyber attacks are waged against a wide variety of targets on millions of computers and networks around the world. These battles rage twenty-four hours a day, seven days a week each and every day of the year. This has led to a flurry of new cyber units within the intelligence and military world, and with this, of course, comes job opportunities.

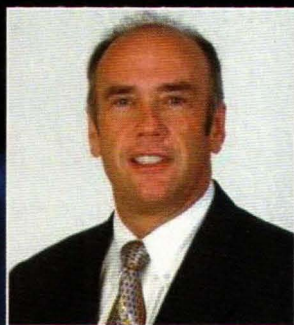


WANTED



CYBER WARRIORS

for the emerging cyber



Kevin Coleman

COLD WAR

Back in the spring of 2007, US Strategic Command Chief General James E. Cartwright told Congress that "America is under widespread attack in cyber space." In addition, officials in Europe have not hesitated to highlight the growing cyber warfare threat.

For many years, observers believed that the balance of cyber war power was tipped in United States' favour. However, there is strong evidence that this has or is changing. China, Russia, Iran and India are quickly closing the gap. Now some experts say the USA is no longer "number one" - it's more like "number three".

The United States has a sophisticated information-warfare programme under the control of the Department of Defense (DoD) and growing cyber defences under the watchful eye of the Department of Homeland Security (DHS). Most military services in the country have focused on using cyber space for intelligence gathering and monitoring. The most advanced is the National Security Agency (NSA). Recently the focus has been expanded to more than intelligence collection and now includes offensive and defensive capabilities as well as for counter-intelligence activities.

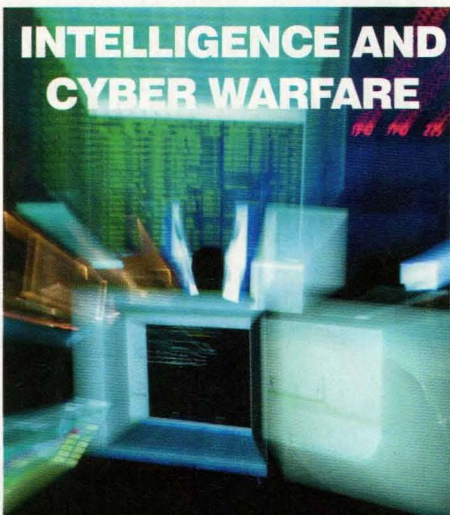
As the cyber warfare threat environment evolves, new career opportunities are created. We have seen a very broad spectrum of positions in the cyber warfare domain. The top three (most frequent openings) are identified here:





Sailors on the watch-floor of the Navy Cyber Defense Operations Command monitor, analyse, detect and defensively respond to unauthorised activity within US Navy information systems and computer networks

INTELLIGENCE AND CYBER WARFARE



INTEL: Last year China graduated around 900,000 scientists and engineers compared to less than 200,000 that graduated in the United States.

INTEL: Spy-Ops, a special training company recently announced its second graduating class of their Certificate in Cyber Warfare programme

INTEL: Recent cyber attacks appear to be an attempt take advantage of an ongoing political and economic crisis.

INTEL: The United States military is more reliant on computers and networks than any other military in the world today.

INTEL: China had 210 million Internet users at the end of 2007 and the online population is thought to have become the largest in the world in 2008.

a few interesting facts

CYBER INTELLIGENCE ANALYST

Responsible for reviewing and assessing all cyber intelligence gathered by various intelligence agencies and conducting analysis and production of intelligence reports. In addition, the position will identify intelligence gaps in reporting and provide constructive feedback to enhance intelligence gathering performance.

CYBER OPERATIONS DIRECTOR

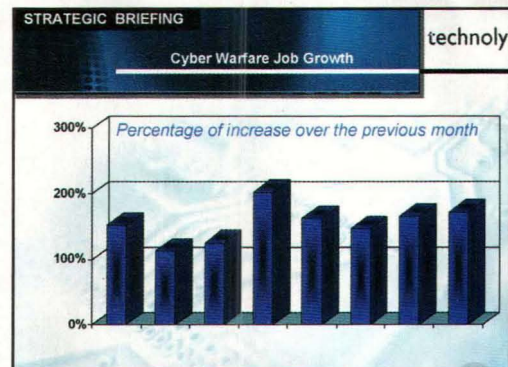
This position is for developing strategies for cyber warfare operations, plans, goals, objectives, priorities, missions, and timelines to execute cyber warfare missions. An officer-level position will assist in planning and directing actions for the full range of cyber weapons deployment against computers and network operations.

CYBER WEAPONS SPECIALIST

Provides technical direction within a team of software developers, software engineering and systems integration personnel that create innovative offensive cyber attack capabilities. In addition, the responsibilities will include identifying and developing cyber software that provide a strategic advantage in the area of Cyber Warfare/Information Operations.

One source inside the DoD told me that cyber weapons and defense systems require our service personnel to receive current and relevant training and maintain their level of competency as the threat environment changes. This ensures they are capable of fighting and winning within the domain. Education and training are the foundation for security in this highly technologically advanced military environment. However, this is a huge challenge, not only for the USA and UK, but for many other countries as well. These resources are in high demand in the corporate world (private sector) and the increased demand from

© SPY-OPS



the military and government (public sector) will make attracting and retaining these resources a challenge.

A military organisation's ability to be successful in the continuous evolving and technically challenging cyber threat environment depends on highly educated resources at all levels. And this is even more the case in the cyber warfare domain. A Spy-Ops associate tells us that "a new breed of military officer needs a broad based training programme in the cyber area in addition to particular area of expertise." He went on to explain that cyber training must

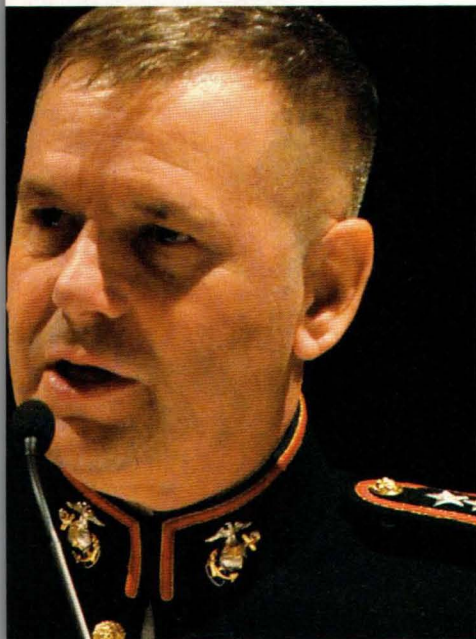
"America is under widespread attack in cyber space..."

US Strategic Command Chief General James E. Cartwright

broaden our understanding of cyber weapons and strategies and contribute to other military operations that may be used in conjunction with traditional attacks.

CYBER UNITS

Multiple branches in the DoD, for example, have established a professional cyber force and are developing multiple cyber career paths for officers, enlisted personnel and civilians. In addition, the National Guard has reportedly joined this effort and has made the plan a focal point for future recruitment. It's also hoped the government's stimulus package and the recent announcement of a 60 day information infrastructure security assessment will also drive demand for these resources.



CONCLUSION

As the "cyber cold war" heats up, the demand for these highly skilled resources will increase. The educational requirements coupled with the ability to obtain a security clearance will combine to make this a challenge for military leaders around the world.

When you factor in the demand from the business community, the challenge becomes huge. This problem is not unique to the United States. Our analysis suggests that over 30 countries, including the UK, will face a severe shortage of technical talent needed to address the threat of cyber war.

© KEVIN COLEMAN/SPY-OPS 2009

UK

UNDER CYBER ATTACK

e-mails go east as computer virus strikes military systems

The Ministry of Defense (MOD), has begun to investigate what has been called the most significant cyber security breach ever after information and evidence surfaces that e-mails sent from multiple Royal Air Force (RAF) stations were sent to IP addresses traced back to Russia.

A hybrid computer virus/worm was allegedly able to penetrate MOD system security in January. An MOD spokesman reportedly said that "action was immediately taken to isolate the infected systems and commence virus-cleansing procedures to protect from re-infection."

This security event resulted in the need to bring down systems and halt much e-mail communication across the military. Reports that the Royal Air Force had some of their systems impacted as well remain unconfirmed at this point.

Digital DNA analysis of the sophisticated virus suggest that it originated somewhere in the former eastern bloc. The impact of the computer virus attack was significant. The MOD stated that the performance of its IT systems had been affected by the computer attack but would not elaborate further.

Other reports suggest that over 24 RAF bases and 75% of Royal Navy ships - including the

aircraft carrier HMS Ark Royal - systems were infected/impacted. Some of the media speculated that the stations attacked by the worm were ones that would be used to scramble aircraft for Russian bomber intercept.

This incident came on the heels of a similar attack on the Pentagon in the United States. Could this be the same bug? Cyber security experts say they appear to be similar but are not willing to say they were identical. The computer virus caused the Pentagon to ban the use of USB memory sticks or flash drives.

Although the US Department of Defense has not provided any official comment on the attack on their UK ally, one thing is clear, cyber attacks have accelerated and many believe we are on the verge of an all-out cyber war.

News of the UK incidents broke after an alleged official, concerned that not all necessary steps to secure systems are being taken, spoke to a politician. The MOD firmly denied knowledge of any e-mails being sent to a Russian.





KEYKATCHERS

ALL
COMPATIBLE
WITH MACS

KEYKATCHER's new range of the world's most popular and best-selling key loggers. Unbeatable quality, highly versatile and undetectable... covert monitoring of all computer activity

Please use order form on page 82 or call Eye Spy direct



KEYCARBON CORPORATE SE

Order code: ES-KC-COR
UK £155.00 USA \$270.00
ROW £165.00

KEYCARBON FORENSIC

Order code: ES-KC-FOR
UK £199.00 USA \$360.00
ROW £210.00

KEYCARBON HOME

Order code: ES-KC-HOM
UK £120.00 USA \$199.00
ROW £127.50



KEYCARBON USB 1.5MB CORPORATE SE

KEYCARBON USB CORPORATE SPECIAL EDITION: The ideal key logger for all your internet monitoring needs. CAN'T be detected by anti-virus or anti-spy software. This stealthy USB keylogger works on USB keyboards (including wireless) for PC and MAC computers. KeyCarbon records every keystroke typed on your computer (over 1 million keystrokes) including e-mail, chat, IM, internet addresses and more. The KeyCarbon USB key logger is the perfect solution for monitoring your employees' computer and online activities. A KeyCarbon keylogger is the easiest way to monitor your PC or MAC. Simply unplug your keyboard and plug the KeyCarbon into the USB port. Then plug the keyboard into the KeyCarbon and it's ready to record. There is no software to install. As keys are typed the data is stored inside the device. When you want to see what's been recorded simply open any word processor or text editor (Microsoft WordPad recommended) and type your password. The KeyCarbon keylogger will display a menu allowing you to view what's been recorded. **AVAILABLE IN BLACK OR WHITE.**

System Requirements: USB keyboard connector (works with both high & low speed USB).



KEYCARBON USB 2MB FORENSIC

KEYCARBON USB FORENSIC KEY LOGGER : NOW WITH TIME/DATE STAMPING: Functions and description like the above but records over 2 million keystrokes and comes with date and time stamping allowing accurate forensic investigation. Perfect for specialist investigative operations and long-term monitoring. Cross reference users with activity.

KEYCARBON USB 512K

KEYCARBON USB HOME KEY LOGGER: Functions and description like the above (no time/date stamping) with recording capacity of over 512,000 keystrokes. The perfect low-cost solution for monitoring your child's on-line activity.

KEYKATCHER HARDWARE KEYSTROKE RECORDERS FOR HIGH-USE FAMILY COMPUTER MONITORING

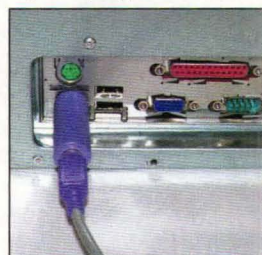
All keystroke loggers are literally an anti-virus software update away from becoming obsolete! KEYKATCHERS CANNOT be DETECTED or DEFEATED by anti-spy software programmes. Our 256K key logger stores over 162,000 keystrokes including e-mail, chat, IM, internet addresses and more. We recommend KeyKatcher key loggers for professional use, for homes with high levels of computer activity or for any application requiring infrequent checking. The new Magnum KeyKatcher has a fantastic 4MB capacity and also date and time stamping for forensic and specialist use. For our full range - visit www.eyespyimg.com (shop).

- Search capability
- Memory remains intact even when unplugged or during power loss
- No software to install
- Virtually undetectable
 - Will defeat all electronic and software bug hunters

System Requirements:
PC and MAC compatible computer

For more KeyKatcher products and further information visit:
www.eyespyimg.com

Magnum KeyKatcher



KEYKATCHER MAGNUM 4MB

MORE UNIQUE FEATURES & HIGHEST MEMORY CAPACITY OF ANY PS/2 HARDWARE KEYLOGGER ON THE MARKET: 128-Bit Encryption, Time/ Date Stamping, Time of Use Charts, 4 Megabytes of Data Storage, TrueStampTM Technology makes it virtually impossible to falsify time/ date stamps. This extra level of security leaves no doubt about when activity occurs. Records Data at the Source - KEYKatcher keyloggers records keystrokes as they are typed for maximum accuracy and reliability. Software is vulnerable to detection and being deleted. Quick Erase - Erasing memory takes about 4 seconds - faster than other KEYKatcher products. Multiple Viewing Options and a customizable password allows you to change the password from the default to a password of your choice. Magnum's powerful search utility allows you to search the memory without downloading the data. Searches save time and allow you to quickly piece together activities.

KEYKATCHER MAGNUM 4MB Order code: ES-KK-MAG UK £92.50 USA \$160.00 ROW £99.00

KEY KATCHERS Can't be detected or defeated by anti-virus software. They also work on wireless keyboards



KEYKATCHER PRO - 256K HARDWARE KEYLOGGER

Records ~128 pages of typing; NETPatrol & Keyword, search facility
Order code: ES-KKPRO UK £55.00 USA \$1000.00 ROW £65.00

KEYKATCHER FAMILY - 128K HARDWARE KEYLOGGERS

Records ~ 64 pages of typing - Internet monitoring no software
Order code: ES-KK5 UK £50.00 USA \$90.00 ROW £60.00

KEYKATCHER MINI - 64K HARDWARE KEYLOGGERS

Records ~ 32 pages of typing - Internet monitoring no software
Order code: ES-KK4 UK £46.00 USA \$60.00 ROW £55.00

KEYKATCHER USB ADAPTOR SET

The USB adaptor set allows KEYKatcher products to work with most USB keyboard set-ups. If your USB keyboard shipped with a PS/2 adapter, the adaptor set will work with your system. If your keyboard did not ship with an adapter, please check your documentation to see if your USB keyboard will work with a non-active PS/2 adapter.

Order code: ES-KKAS
UK £25.00
USA \$25.00
ROW £30.00



EYE SPY CLASSIFIED

Eye Spy Intelligence Magazine Classifieds. All inserts appear in 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 go to www.eyespyimag.com and download our media pack. Similarly you can write to our USA, UK or Canadian address.

Payment must be submitted prior to publication.
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.

**FOR A QUICK QUOTE CALL UK: 01756 770199
USA TOLL FREE 877 309 9243**

INTERNATIONAL, CORPORATE, PRIVATE, PROFESSIONAL, SURVEILLANCE, TRAINING,
EQUIPMENT, PHOTOGRAPHIC, SPECIALIST, SECURITY, INVESTIGATION

TRAINING AND SECURITY



The GIA Group Ltd

Global Intel Associates

www.giaintel.com



BLACKCHRYSALIS

BLACKchrysalis is a unique specialist security and intelligence agency, specialising in covert operations, protection and confidential business consultancy and instruction to civilian, government and foreign military clients.

www.blackchrysalis.com



Producers of the acclaimed surveillance DVD

AM I BEING WATCHED?

See page 55 for details



Athena

Security & Intelligence Consultants Ltd

Advanced Hostage Negotiation Training Course (12 Days)

Our course trains Security and Security Force personnel to conduct the delicate and emotive negotiations required to maximise the potential of a successful outcome to a difficult and turbulent situation.

Taught by experienced former Metropolitan Police Negotiators, individuals are trained to UK National Police Course standards to deal effectively with all manner of siege and kidnap scenarios including Suicide Intervention, Criminal and Terrorist Hostage Takers as well as Maritime Piracy.

Courses are taught in English, but Interpreters can be provided, if required.

Course fees start at £4000 + VAT per Student (costs may vary if Students are accommodated on-site or if Interpreters are required). Courses can be held in the UK or overseas subject to Client requirements.

For further information, please visit
www.athenaintelligence.co.uk or telephone
+44 (0)141 314 3983



Athena

Security & Intelligence Consultants Ltd



KIDNAP AVOIDANCE AND HOSTAGE SURVIVAL TRAINING

Essential, life-saving training for any individual, or responsible agency with personnel working or travelling in potentially hostile environments.

'...the best training of its type I have seen in my 20 years of service'.

Senior European Police Officer

There are over 20,000 reported kidnapping incidents worldwide every year.

The sad fact is that many Kidnap for Ransom cases could have been avoided.

If a kidnapping occurs – there are many things that can and should be done to ensure the speedy, safe return of the Captives to their loved ones.

With correct training...

- **YOU CAN** reduce the chance of being kidnapped in the first place.
- **YOU CAN** positively affect the outcome of any Hostage situation.
- **YOU CAN** minimise the risk of unnecessary harm befalling you or other captives.
- **YOU CAN** maximise the chances of returning home to your loved ones in the shortest possible timeframe.

Key Speaker—Simon Atkinson, is a former UK Forces Special Intelligence Officer who was instrumental in the design and dissemination of the UK Hostage Awareness and Survival policy. Having been intimately involved in the safe recovery of Hostages, he has appeared on national news stressing the importance and benefits of suitable training for individuals or companies who may fall victim to this pernicious industry.

Programme Includes:

- Avoiding the Risk
- Surviving Captivity
- 1st Responder—Negotiator Training
- Denying Time-Sensitive Information
- Remaining Safe During Rescue

Who Should Attend?

- Security Professionals
- Potential 'Lone Travellers'
- NGO/Overseas Charity Staff
- Journalists
- Employers, demonstrating 'Duty of Care' in the light of the Corporate Manslaughter and Homicide Act 2007.

For registration details, please email events@athenaintelligence.co.uk or call +44 (0) 141 314 3983



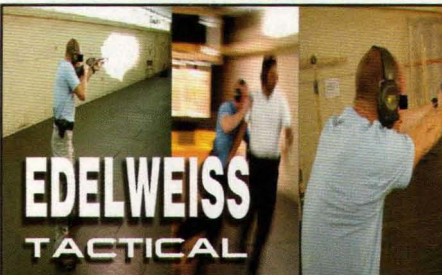
ISS Training Ltd

ISS Training Ltd,
Riverside Cottages,
Nidd Walk, Pateley Bridge,
Harrogate,
North Yorkshire, HG3 5NA, UK
Tel: + (0) 1423 712265
info@intelsecurity.co.uk

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

Specialists in delivering industry recognised, accredited and non-lethal training courses to professional personnel working in the security industry

THE WORLD'S PREMIER SURVEILLANCE PROVIDERS



EDELWEISS TACTICAL

certificated firearms training

For more details visit
www.edelweisstactical.com
or www.intelsecurity.co.uk or telephone
ISS + (0) 1423 712265 UK



0800 975 4939

www.futureglobal.co.uk

BUSHCRAFT
Courses and Training
YOU CAN SURVIVE

- Fire lighting • Trapping
- Search and Rescue
- Shelter Building
- Living off the Land
- Knifecraft • Navigation
- Tracking • Archery
- Wilderness First Aid
- Shooting • Team Building



For course details contact Head Instructor
Mike Armstrong UK 01535 634685
or e-mail: info@bushtruck.co.uk

INVESTIGATION SPECIALISTS

www.locateuk.com
Private Investigators

Technical Surveillance Countermeasures
Tel: 02079936047 Fax: 02030519447
email: info@locateuk.com

DAY AND KNIGHT INVESTIGATIONS LTD

www.dayandknightinvestigations.com

S FISHER SERVICES

• SECURITY • INVESTIGATIONS • SURVEILLANCE

Telephone 07866 010363 UK
e-mail e7hsf@yahoo.co.uk SIA Registered

SECURITY PRODUCTS

www.encrypted-call.com

secure gsm mobile phones

protect your private phone calls from intrusive surveillance.

call : **0845 050 6533**

READING THIS?

Your advert here for just
£30.00 (\$45.00)!

CALL + 44 1756 770199
UK FOR MORE INFORMATION

INTELLIGENCE TRAINING

technolytics

Technology for Intelligence

follow... or be pushed aside?

www.technolytics.com

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.

www.Spy-Ops.com

SECURITY TRAINING BOOKS

• **TRADECRAFT** •

COVERT SURVEILLANCE AND INTELLIGENCE GATHERING
Eye Spy Ref: ES/GIA1 £55.00 \$110.00

GAINING INTELLIGENCE AND EVIDENCE FROM COMPUTERS
Eye Spy Ref: ES/GIA2 £65.00 \$125.00

BUY BOTH BOOKS Eye Spy Ref: ES/GIACOMBO £110.00 \$200.00
Please use order form on page 82

THE MODERN BODYGUARD

FULLY REVISED

AVAILABLE FROM EYE SPY

The Modern Bodyguard
Peter Consterdine

ORDER CODE: ES1213
UK £25.00 USA \$50.00 ROW £30.00

Please use order form on page 82

ADVANCED SURVEILLANCE
The Complete Manual of Surveillance Training
by Peter Jenkins

ADVANCED SURVEILLANCE
"Everything you ever wanted to know about surveillance..."

AVAILABLE FROM EYE SPY ORDER
CODE: ES712 UK \$25.00
USA \$50.00 ROW £29.99
Please use order form on page 82

INTELLIGENCE AND SECURITY WEB SITES

EYE SPY
THE COVERT WORLD OF ESPIONAGE AND INTELLIGENCE

www.eyespymag.com

STRATFOR

Global Strategic Intelligence

GlobalSecurity.org
Reliable Security Information
www.globalsecurity.org

MUSEUM WEBSITES

CAMP X
Visit Canada's famous WWII special agent training camp museum
www.camp-x.com

BLETCHLEY PARK
National Codes Centre

FINLAND'S SPY MUSEUM
www.vakoilumuseo.fi/

ORGANISATIONS & SOCIETIES

OSS www.ossociety.org

AIR AMERICA
www.air-america.org

ENIGMA 2000
Number Station Monitors Group
<http://groups.yahoo.com/group/enigma2000>
for Analysis, Prediction and Log Data

• DESIGN • DOMAIN • e-COMMERCE
• TECHNICAL SUPPORT
• ACCESS TO e-stock-eyespy PHOTOS

ESPL
Builders of web sites for the security and corporate world
from £100.00 to £10,000

For further information write to
ESPL, P O Box 10, Skipton,
Leeds City Region, BD23 5US, UK

CONFERENCES • LECTURES • EVENTS



CHRIST CHURCH, OXFORD CONFLICT CONFERENCE 2009

The Making of the Modern Middle East

Sunday 6 September – Friday 11 September 2009

Christ Church, Oxford is home to the autumn series of conferences on the theme of conflict. This, the seventh event in this well established series, is run in collaboration with the University of Oxford's renowned Middle East Centre, and takes as its theme the enduring and apparently intractable confrontations of this region.



Christ Church
OXFORD

For further information please contact:
The Making of the Modern Middle East
The Steward's Office
Christ Church Oxford ox1 1dp

Tel: 01865 286848/286877
Fax: 01865 286328
Email: conflict@chch.ox.ac.uk
www.chch.ox.ac.uk

www.coldwar.org

COLD WAR MUSEUM

MISCELLANEOUS

Defence-Guide.com
Worldwide Military Guide for Army, Navy and Air Force

PHOTOGRAPHIC SPECIALISTS

News agencies/media
- need a photographer in London?
SNAPPERJACK
available 24-hours-a-day...

UNDERGROUND

SNAPPERJACK of London
www.snapperjack.net



SUPPLIER OF REAL-TIME IMAGERY TO THE TRADE AND
EYE SPY INTELLIGENCE MAGAZINE

Tel. 020 79936047
Fax. 020 30519447

PUBLICATIONS

OSS SOCIETY Journal
Fall 2008 Volume 1 No. 1

Also In This Issue:
Subscribe to the new Office of Strategic Services Journal

SPY STORES

WWW EYE SPY mag.com

OVER 2,000 PRODUCTS
serving the trade and public

www.eyespymag.com

Online SPY Shop.co.uk **CALL US ON 0870 977 0661**

• SPYPHONES • COMPUTER MONITORING
• COVERT TRACKING • DELETED TEXTS
• SKELETON KEY (REMOTE ADMINISTRATION TOOL)

www.onlinespyshop.co.uk

TAKING PICTURES

Section 76

Counter Terrorism Act

Continued from page 27

A Downing Street statement released about the photography law is also somewhat vague. There are apparently "no legal restrictions on taking pictures in public places," but states "the law applies to photographers as it does to anybody else." The statement goes on: "So there may be situations in which the taking of photographs may cause or lead to public order situations, inflame an already tense situation, or raise security considerations. Each situation will be different and it would be an operational matter for the police officer concerned as to what action should be taken."

I would hate to think that any of Eye Spy's responsible associate photographers could be



Photographers protest outside New Scotland Yard

arrested for simply taking a picture of MI6 headquarters, for example.

And it's precisely that last point that worries many in the trade. It's a law open to interpretation, but I hope it's one sensibly managed.

New Scotland Yard are altogether more astute in their analysis of Section 76, especially senior officers. Officials here insist the law was brought in to help protect counter-terrorism officers. They also note that any prosecution would have to be in the public interest. "For the offence to be committed, the information would have to raise a reasonable suspicion that it was intended to be used to provide practical assistance to terrorists. Taking photographs of police officers would not, except in very exceptional circumstances, be caught by this offence."

Yet fringe groups opposed to any restriction have already said they will not adhere to the

law. Leo Murray is a spokesman for climate change campaign group Plane Stupid. This outfit usually film their actions. "It's outrageous," he told the BBC News website. "It's yet another in a long line of measures designed to erode people's civil liberties. Being able to film the police has completely changed the way they are able to police our protests. It's made us much, much safer and the risks of a violent confrontation have almost disappeared. If we couldn't film they could act with impunity, they could just mete out violence with the confidence that nobody would find out. There's absolutely no way we are going to observe this ban. If they try to bring charges against us we will fight them in the courts."

Few would bet against someone ending up in court in 2009 charged under Section 76 of the Act.

Editor - Eye Spy



OFFICIAL EYE SPY ORDER FORM 2009

ref	price	ref	price

name _____

address _____

post/zip code _____ country _____

method of payment [A] cheque [] [B] credit card []

Cheques/Postal Orders payable to: 'EYE SPY PUBLISHING LTD'

card number _____

expiry date _____ Last 3-digits on reverse of _____

issue number (Switch UK only) _____ card (security code) _____



total £ or \$



UK, EUROPE AND REST OF WORLD



Eye Spy Magazine, P.O. Box 10,
Skipton, Leeds City Region, BD23 5US, England
Or Telephone: 01756 770199 (UK) standard rates



UNITED STATES OF AMERICA

Eye Spy Magazine, Empire State Building,
350 Fifth Ave, Suite 3304-22H, New York,
NY 10118-0069, United States of America
Or Telephone TOLL FREE 877 309 9243



CANADA

Eye Spy Magazine, Canadian Bureau
P.O. Box 153, Port Perry, Ontario,
Canada, L9L 1A3
Or Telephone TOLL FREE 877 309 9243

WE ACCEPT ORDERS VIA PAY PAL eyespy@eyespy.com

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, Leeds City Region,
BD23 5US, England
Telephone: 01756 770199
e-mail: support@eyespyimag.com
Web Site: www.eyespyimag.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

editors, consultants and feature writers



Michael Smith associate editor	Kevin Coleman USA associate editor	Mark Birdsall managing editor	Lynn Hodgson canadian editor	Peter Jenkins senior surveillance editor
Kerap Gourdikian associate editor	David Hamer associate editor	Danny King security consultant	John-Hughes Wilson consultant	Adrian Radford consultant
Nick Fielding senior consultant	Jay Goldberg security consultant	Spiros Koplissos security editor	David Bickford senior intelligence consultant	Glenmore-Trehear-Haney associate editor

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.

SUBSCRIPTIONS

united kingdom	\$27.50
united states of america	\$49.99
europa	\$30.00
Canada	C\$60.00
australia/middle east/asia/africa	\$30.00

please make cheques payable to:
Eye Spy Publishing Ltd

Classified Place Advertising:
UK 01756 770199
USA Toll Free 877 309 9243

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

Registered Company No. 4145 963 Registered for VAT: ISSN 1473-4362

EYE SPY functions solely as an independent, investigative and reporting organ only; it is non-political and does not discriminate against colour, race, religion or creed. Points of view to the editor please.

ISTICOR

NORTH AMERICAN DISTRIBUTION

UNITED STATES OF AMERICA & CANADA -
Toronto: 905-619-6565

magine

UK • EUROPE • ROW DISTRIBUTION

UK, Europe, Australasia, Rest of World
Imagine: UK 0845 612 0094

COMING SOON TO

EYE SPY

TRADING PLACES

WHEN INTEL COLLECTION
IS JUST TOO DANGEROUS
FOR CIVILIAN AGENCIES

ISSUE 62 ON SALE LATE APRIL/EARLY MAY



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

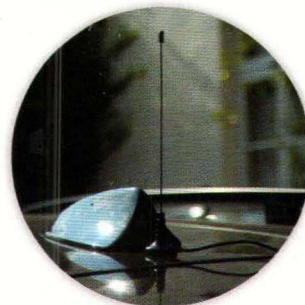
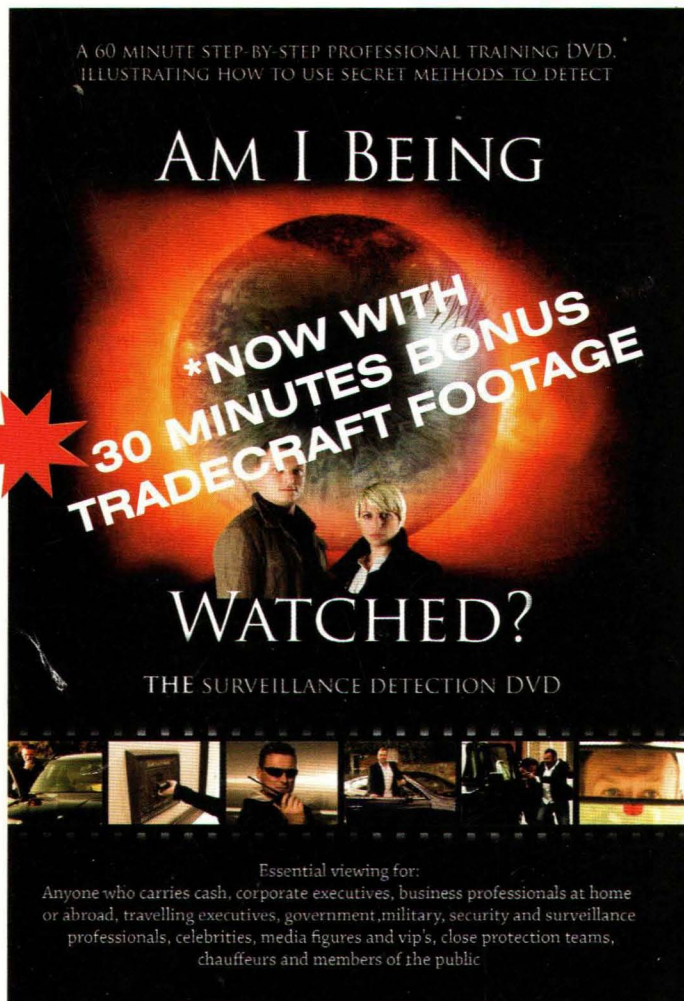
FILMED ENTIRELY IN
SUPER HD

ESSENTIAL VIEWING

AM I BEING WATCHED?

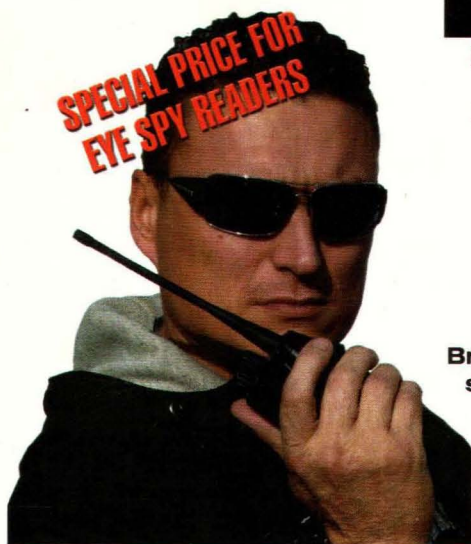
A 60* minute step-by-step professional training high-definition DVD illustrating how to use secret methods to discover...

for government, military, security and surveillance professionals, close protection teams, media figures, corporate and travelling executives, business persons, chauffeurs, celebrities and importantly - members of the public



Each DVD contains
discount (£5.00/\$10.00)
voucher for Volume II

SPECIAL PRICE FOR
EYE SPY READERS



Before an attack, theft, kidnap or an attempt to gather information about you, your family, business, home or office, one thing is proven... your routine will be watched.

Learn all the secret skills used to identify surveillance without anyone knowing you are even looking... this is the art of anti surveillance.

In this highly informative, instructional and professional DVD, ADRIAN RADFORD, a former British intelligence instructor presents some of the secrets of this essential guide to discover if you are being watched

Am I Being Watched DVD - EYE SPY Special Reader Offer: UK £39.99 • USA \$79.99 • ROW £45.00
Usual Price: UK £49.99 USA \$99.99 ROW £55.00 WORLD
Ref: DVD-ES1 please use order form on page 82. Overseas orders sent air mail

Am I Being Watched - is part one of a professional three DVD series on anti-surveillance, countersurveillance and related tradecraft and security issues. It is produced by BLACKChrysalis and distributed solely by Eye Spy Publishing Ltd. Outlets should contact Eye Spy for trade questions and reselling licences.