

THE COVERT WORLD OF ESPIONAGE

EYE SPY

82 SECONDS
LONDON TERROR ATTACK



CIA LISTENERS

ENTRAPMENT
A DANGEROUS TRADecraft

FEMALES &



INTELLIGENCE



ASSASSINS
OF OFFICE 225

- ALTERNATIVE HACKING • MI6 RECRUITERS • US INTEL-WHITE HOUSE WAR
- TRUMP'S WATERGATE • NEW UK CYBER CENTRE • CIA RENDITIONS
- MOSCOW UNDERWORLD • AIRLINE DECEPTION • ISIS BOMB PLOT

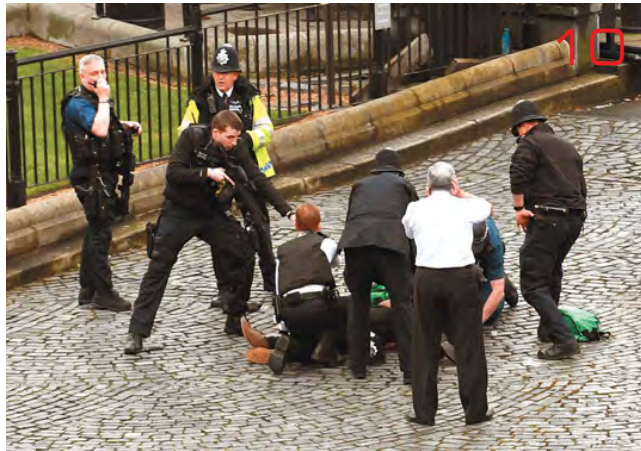


NUMBER 108
2017
£3.95

Printed and Published in Great Britain



82 SECONDS



ISIS-inspired terrorist strikes in the heart of London using vehicle as weapon



As North Korean assassins strike again, Eye Spy examines the country's dark intelligence agencies



Documents Leak Expose Agency Bugging Elements



CHANGING TIMES

Intelligence and security appointments reflect changing dynamics of a domain once totally dominated by males



GCHQ Launches Britain's National Cyber Security Centre

37



ENTRAPMENT



EYE SPY 108



VOLUME XIV NUMBER FOUR 2017 (ISSUE 108)
ISSN 1364 8446 publication date: APRIL 2017
FRONT COVER MAIN IMAGE:
TALISMAN INTELLIGENCE LIBRARY/VARIOUS



MAJOR CONTENT GUIDE

13 NK OFFICE 225 - ANALYSIS

Secret North Korean spy element uses female proxies to assassinate President Kim Jong-un's half-brother in audacious operation in Malaysia

20 PAYBACK: A DARK CONSPIRACY

Several key Russian and American intelligence, military and political figures depart following more allegations of secret liaisons - whilst one alleged contributor to the 'Trump Dossier' is found dead in Moscow

23 LANGLEY'S NOT SO SECRET VAULT 7

WikiLeaks release a plethora of recent top secret CIA material concerning the Agency's electronic bugging arms

27 ENTRAPMENT AND COMPROMISE

A major tradecraft feature covering numerous methods deployed by the intelligence world and others revealing just how easy an individual can fall prey to entrapment

34 INTEL DETENTE

NATO and Russia engage in secret talks as intelligence and military figures warn of possible conflict in Eastern Europe and the Baltics

37 NCSC - INTERNET DEFENCE OF THE REALM

Britain opens its primary cyber defence arm - NCSC (National Cyber Security Centre) - a major directorate of GCHQ

40 CHANGING TIMES

A look at how more and more senior intelligence posts are being filled by woman - this as MI6 embark upon a remarkable recruitment programme targeting females

44 DEEP BLACK

The CIA's extraordinary rendition programme resurfaces to haunt a number of British intel and political figures

50 WATERGATE II: BUGGING OF TRUMP TOWER

President Trump's allegation of eavesdropping examined as former journalist compares affair to Watergate and Nixon

54 AIR DECEPTION

US and UK ban selective electronic media devices from some airline carriers as fear of terrorism spreads

57 ALTERNATIVE HACKING

A fascinating feature exploring the history of alternative hacking - and some operations which were indeed ethical

62 A MATTER OF ASSURANCE

Just days before a terrorist struck on the streets of London, UK security services held a counter-terrorism operation on the River Thames in the centre of the city

57 THE WORLD OF COUNTERINTELLIGENCE PT4

Dr Chris Northcott concludes his indepth examination of counterintelligence and its relevance to security and espionage

72 THE DECEPTIVE FACTOR PT3

Mike Finn looks at the art of distraction and its uses in the intelligence cycle

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

"No Sir, nor would I... that would be expressly against the construct of the Five Eyes Agreement"

On allegation he asked GCHQ to bug Trump Tower



Michael Rogers - Director NSA

FIRST WORD

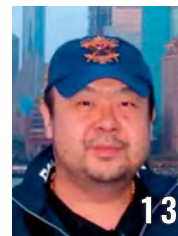
LONDON TERROR ATTACK AND LONE WOLVES



With little planning, no support network and 'armed' with just a hire car and two knives, one attacker brought central London to a shuddering halt. In an action that lasted less than two minutes, Briton Khalid Masood opted to take the lives of four innocent people. Despite the area being a well guarded and heavily fortified location, Masood showed just how vulnerable the public are when a determined terrorist, devoid of all sense of justice strikes. ISIS claimed the attacker was one of its own 'soldiers', but this is not the case. He may well have been 'inspired' by the group's rhetoric, and even influenced by similar events in Nice and Berlin, but senior security officials have found no evidence of direct communication or control - at least not yet.

It's also ironic that the attack occurred just days after a major security exercise involving various organisations took place on the River Thames - in this case the operation simulated a cruise ship hijacking. Police said the event, watched by an invited media - was one of public assurance and preparedness. Yet Masood showed that even with the best security officers and counter-terrorism agencies in the world, not all attacks can be prevented. A most worrying time.

MARK BIRDSALL, MANAGING EDITOR



HEADLINERS



•8 Jeremy Fleming •10 Khalid Masood •13 Kim Jong-nam
•41 Cressida Dick •44 Abdel Hakim Belhaj •54 Ibrahim al-Asiri
•56 Martin McGuinness •82 Denis Voronenkov

INTELLIGENCE CHOICE

LANGLEY, RENDITION AND SECRET LIAISONS

When President Bush decided he was going to find those responsible for attacking the United States in 2001, the CIA embarked upon a global seek and detain quest.

Langley used all its prowess and cunning in an operation which lasted several years. Many of those secretly captured and moved to Guantanamo Bay protested their innocence, but hundreds were involved with the terrorist activities of al-Qaida. Few doubt the CIA received help from several foreign intelligence services, and this liaison has come back to haunt a number of countries...



•44 DEEP BLACK



INTELLIGENCE REVIEW • NEWS • DIGEST

NOT SO SECRET

North Korean Spy Chief Fired

According to sources within South Korea's Ministry of Unification, Seoul's government department responsible for promoting the reunification of the Koreas, NK leader Kim Jong-un has fired his spy chief General Kim Won-hong from his post as Minister for State Security.

General Kim was widely viewed as one of Kim Jong-un's most trusted advisors, until that is, he was dismissed on charges of corruption and abuse of state power. Some reports suggest that his dismissal may be related to the defection of Thae Yong-ho, a senior North Korean diplomat who defected with his family while



General Kim Won-hong
serving in the country's embassy in London last year. Yong-ho was the highest ranked diplomat ever to defect.

ACTION COUNTERS TERRORISM

MAJOR RISE IN NUMBER OF 'LIVE' UK COUNTER-TERRORISM OPERATIONS

Just days after stating the chances of a terrorist attack in Britain have never been greater, an ISIS supporter struck in Westminster (see page 8). New Scotland Yard (NSY) Assistant Commissioner Mark Rowley had revealed the scale of this chilling fact. NSY, MI5 and other organisations, which undoubtedly include MI6 and GCHQ, have 500 live ongoing counter-terrorism operations at any one time. Similarly, he again referenced the fact that the UK security services had "prevented 13 terror plots" in the last three years. A spokesman for MI6 in October 2016, said "twelve attacks had been prevented."

Since March 2016 to March 2017, 22,000 members of the public contacted police to provide information on suspects and suspicious activity - all the data entering the counter-terrorism and related indexes. Mr Rowley

admits, however, that some people are reluctant to make contact because they fear "wasting police time," or are uncertain if what they know or suspect is of high value. He said the police would rather receive the information regardless, and if it turns out to be nothing, "there was no problem... that's fine." Rowley said they would "rather

have many calls like that, than miss out in the critical one that helps us stop an attack."

His comments followed the launch of a new CT endeavour aimed at securing direct public support. Called Action Counters Terrorism, Mr Rowley has called on the public to contact police about their suspicions and if they have any



New Scotland Yard Assistant Commissioner Mark Rowley

evidence or information about possible terrorist planning. According to official data, the public provided assistance in a third of investigations - all within a category described as 'High Risk'. Since 2014, a suspect has been detained nearly every single day in connection with terrorist activity in Britain.

Rowley said the public's contribution was both extraordinary and vital. "Some information is a change in a person's behaviour, other about suspicious activity," he said. He also admitted that at times it is public information that enables an investigation, and/or





Thae Yong-ho

It is also believed that Kim was demoted from a four-star to a one-star general.

Since taking power in late 2011, Kim Jong-un has executed or purged a number of high-level government officials, but until now, has not interfered in the country's intelligence and security agencies. North Korea has not confirmed the sacking, but Kim Won Hong could face harsh punishment once an investigation into his actions is completed.

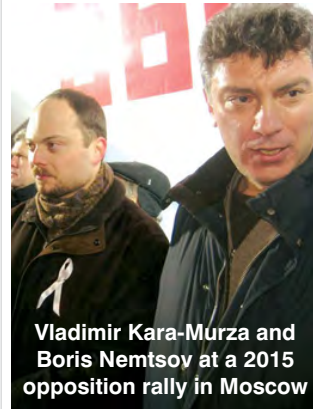
ENEMY OF THE STATE

Long-time Putin Critic Poisoned

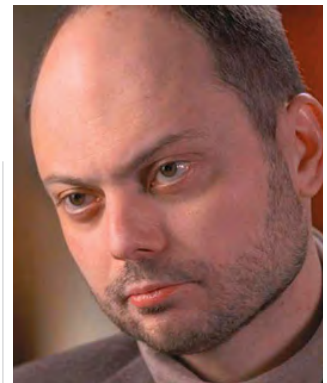
Vladimir Kara-Murza Jr, 35, a politician and officer of Open Russia, a pressure group advocating democracy in Russia, was taken to a Moscow hospital where doctors say his organs failed. His wife says he became critically ill while visiting Moscow and was placed on life support in an episode that mirrors a similar incident in 2015. On both occasions he was visiting Moscow when he suddenly became sick. A part-time US resident, Kara-Murza has called on Washington to impose sanctions against certain Russian politicians.

Doctors diagnosed Murza with "acute poisoning by an undeter-

mined substance." His blood, hair, and fingernails are reportedly being sent to a laboratory in Israel for further analysis. "We want to get some samples tested again to try to determine what this unidentified substance may be,"



Vladimir Kara-Murza and Boris Nemtsov at a 2015 opposition rally in Moscow



Vladimir Kara-Murza

his wife said. He has since left Russia.

After leaving hospital following the 2015 incident, Kara-Murza said, "it was difficult to believe this was just an accident."

Murza was a close friend and associate of Boris Nemtsov, another Kremlin critic who was assassinated in February 2015.



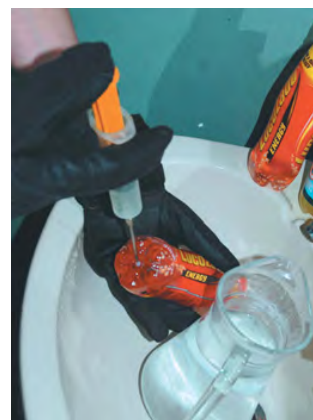
Photo showing New Scotland Yard headquarters (white building) in proximity to Parliament

corroborates what police already know. Noting that at times the public can be a little hesitant to come forward, he urged people to "trust your instinct and don't be cautious."

All the usual terrorist groups were referenced, including ISIS, al-Qaida and the far right, but he warned that the threat could come from multiple places, thus the police needed support from all the public. "We worry about everything from a fairly simple attack

with knives or using vehicles all the way through to more complex firearms attacks," said Mr Rowley.

To coincide with the new awareness programme, NSY has produced a two part podcast - 'Code Severe'. This discusses stories of how terrorist attacks were foiled, interviews with senior officers and participants in the operations, and interestingly, a member of the public explains why instinct helped her decide to contact the police.



Perfect Timing

Kremlin Awaits

LONDON: Britain's Foreign Secretary Boris Johnson has reignited his war of words with the Kremlin, by claiming Moscow has been up to "all sorts of dirty tricks."

In an odd use of words, he said whilst the UK has no evidence the Russians are trying to undermine democracy, "we do have plenty of evidence they are quite capable of doing so."

Mr Johnson referenced cyber attacks in France where a television station ceased operating; the hacking of systems and media in the United States, and for good measure, an assassination attempt of the President of Montenegro.

Mr Johnson is due to visit Moscow shortly.



Boris Johnson

MI6'S MUSICAL CASTRO WATCHER

A 'Pleasant Recruiter' at the Savoy Hotel

There are hundreds of 'celebrity spies' who during times of conflict, war and uncertainty, have opted to help intelligence agencies such as MI6 and the CIA. From John Wayne to Frederick Forsyth, the list is quite a tour de force. Many were selected because of their access to senior figures, travel permissions and... because who would suspect a film star, for example, to be an intelligence collector?



Adam Faith

Now it appears another well known British artist can be added to the collection. Adam Faith was a popular 1960s and '70s singer and actor, who, according to his producer and very close friend, David Courtney, received a visit from an MI6 officer.

Speaking to the *Sunday Times*, Courtney recalled a meeting in 1997 with Faith at the Savoy Hotel in London. As he made his way to the table where his friend was sitting, he noticed him chatting to a man. He was asked to sit at another table while the discussion took place.

Once the meeting ended, Courtney asked: "What was all that about?" Faith replied: "Well, I am going to tell you... but you must not repeat it" Faith explained he was filming a travelogue in Cuba for the BBC and that the mystery man was from MI6. "They approached me and said they knew I had built up some connections in Havana and they



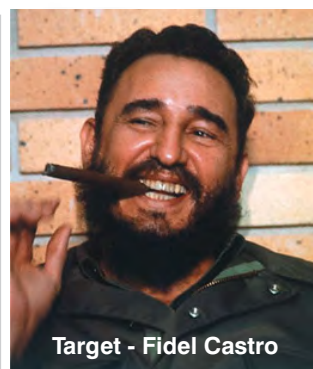
Adam Faith in the 1960s

asked me to do some work for them; basically spy for them in preparation for the post-Castro era." At that time of course, seven years had elapsed since Cuba's Communist protector, the Soviet Union had collapsed.

Just what Faith 'collected' for MI6 remains unknown, but the likable Faith (real name Terry Nelhams-Wright) did go on to meet Castro. Castro asked, "what do you want



The Savoy Hotel, London. A one-time popular meeting place for intelligence officials

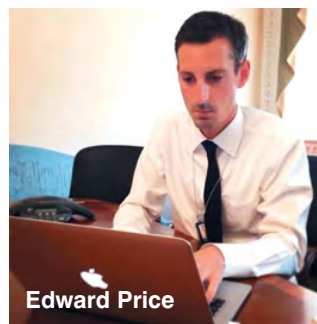


Target - Fidel Castro

NO CIA STAFF EXODUS

Resignation of CIA Analyst Sparks Speculation and Rumours of White House-Langley Rift

Edward Price, a former CIA analyst, resigned citing an inability to serve President Donald Trump's administration because of Trump's policies and what he called a "disregard for the United States Intelligence Community (USIC)." He added



Edward Price

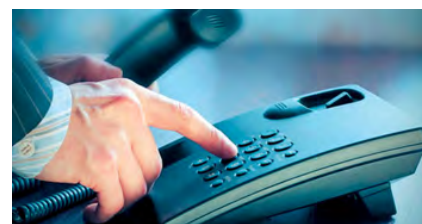
that his resignation had nothing to do with politics.

In actuality, Price was a member of the Obama National Security Council (NSC) staff, apparently on a detail assignment from the CIA. That in itself raises questions as to why a CIA employee assumed an extremely partisan job.

Price's NSC role was to serve as a spokesman and help Deputy National Security Adviser Ben Rhodes run the Obama 'echo chamber' - an organisation that reportedly misled the news media, Congress and the American people about the July 2015 nuclear deal with Iran. Price is alleged to have bragged to *New*

York Times writer David Samuels about how he manipulated and provided flawed information to the press to promote the Iran deal.

Price contributed a total of \$5,000 to the Clinton campaign and the Democratic Party in 2016. This was a huge contribution for a government employee and some observers allege, Price was "angling for a senior job in a Clinton



administration." In addition, Price is a fellow with the Truman Project, a 'left-wing think tank' that served the Obama administration, and he worked for several Democratic political campaigns.

Price's critics point out that if he was an ethical, non-political CIA officer, his resignation could have followed the CIA 'crafting' of politicised talking points on the Benghazi



CIA Director Mike Pompeo



Hiding in Plain Sight

White Coat Distraction

SIS terrorists wearing white laboratory/medical coats attacked patients, staff, visitors and security officers at Sardar Daud Khan Hospital (military) in Kabul, killing at least 49 people and wounding 76.

The attack, which occurred on 8 March at the 400 bed facility in the city's diplomatic quarter - close to the US Embassy - began when a suicide bomber blew himself up at a rear entrance. A six-hour siege then followed.

A further four gunmen, armed with AK-47's began shooting patients and guards floor by floor. At least two explosions were heard, one a car bomb in the



hospital car park; another thought to be an attacker who detonated an explosives' suicide vest.

Security forces were dropped on to the rooftop from helicopters and engaged the attackers killing the remaining assailants. ISIS



claimed responsibility for the attack in a statement carried by its so-called 'Amaq' news agency.

It later transpired that two of the terrorists were hospital interns.

- In 2016, at least 41 attacks on health care facilities and workers were recorded across Afghanistan.

if you don't want money," which just happened to be the title of a popular Faith record. Privately, he also expressed his fears in the event Cuba had learned of his MI6 liaisons.

As for the identity of the MI6 recruiter, Courtney described him as a "pleasant unassuming chap."

- Adam Faith died in 2003, aged 62.

terrorist attacks in 2014. In this case, many intelligence watchers believe the Obama administration pressurised CENTCOM intelligence analysts to slant their analysis towards the ISIS theory.

Intelligence analysts agree that the timing of Price's resignation appears to suggest it had everything to do with politics.

As for the impact on White House-Langley relations since Trump took office, CIA spokesman Dean



ISIS released this image of the attackers

Boyd said there has not been a 'spike' in departures and a former senior CIA official agreed, adding that "people are watching and waiting," giving new CIA Director Mike Pompeo a chance.

Price denies any partisan motivations for speaking out, stating he is not sure what comes next, other than that he hopes to continue serving his country.



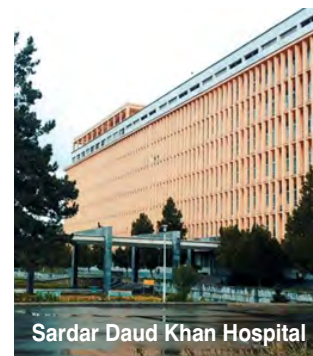
INTELLIGENCE WORK

Saudi Official Honoured by CIA

New CIA Director Mike Pompeo has presented Saudi Arabia's Deputy Prime Minister and Interior Minister, Crown Prince Mohammed bin Nayef, with one of America's most revered intelligence awards.

In a ceremony held in Riyadh, the crown prince was given the George Tenet award in recognition of the Saudi Royal's intelligence work. Pompeo noted his "excellent intelligence performance, in the domain of counter-terrorism and his unbound contribution to realise world security and peace."

Mr Bin Nayef said his country had thwarted several terrorist plots in



Sardar Daud Khan Hospital



recent times, including a number targeting friendly nations. "Combating terrorism requires a joint international effort at all levels; financially, intellectually, militarily and through the media," he said.

Describing the US-Saudi relationship as "strong and historic," the Crown Prince warned his country is "surrounded by areas of conflict."

ALL CHANGE AT GCHQ

New Head is Deputy Director-General of MI5

One of the most important positions in world intelligence has been filled by a man who shares the surname of an intelligence officer who is forever embedded in spylore - Ian Fleming.

Jeremy Fleming, a 24-year intelligence and security veteran who served both MI5, the Security Service, and the Office for Counter Terrorism, is the new Director of Britain's signals intelligence agency - GCHQ. His

appointment follows Director Robert Hannigan's January 2017 decision to step down. Mr Hannigan cited family reasons for his departure.

Foreign Secretary Boris Johnson, who made the announcement of Fleming's appointment, said: "I know he will continue the excellent work of Robert Hannigan in leading this outstanding organisation, when the skill and ingenuity of the UK Intelligence Community (UKIC) are critical to defending Britain from



© MI5/CROWN COPYRIGHT

Jeremy Fleming

cyber attacks, terror plots and other activities that threaten us and our allies."

Outgoing Director, Mr Hannigan, who played an important role in the creation and development of Britain's new National Cyber Security Centre (see page 36) said: "I'm delighted that the Foreign Secretary has appointed Jeremy Fleming to be the new Director. I've known Jeremy for many years and he is a good friend and colleague. He comes with deep intelligence experience and expertise." Indeed, Mr Fleming is a specialist in counter-terrorism, counter-espionage and has much experience in cyber affairs - undoubtedly one reason why he secured the post.



Robert Hannigan, though serving as Director of GCHQ for just a short period, has overseen many changes at the organisation

© GCHQ/CROWN COPYRIGHT

Spymaster MAXWELL KNIGHT

Legendary intelligence officer's life story set for small screen

Henry Hemming's *M: Maxwell Knight, MI5's Greatest Spymaster*, is a book that tells the pulsating story of Knight, a maverick intelligence officer who confronted and disabled British fascism during WWII. Known to his agents and colleagues as 'M', Knight would later be one of the inspirations for the 'M' character in Ian Fleming's James Bond novels.

Mammoth Screen, the group behind such shows as the popular BBC drama 'Poldark' and ITV's 'Victoria', has optioned the film and television rights for the book, which tells the true story of the former MI5 Director of Intelligence.

The work is being developed primarily for television, with a view to producing a multi-part drama that could run up to three



seasons. 'Bridge Of Spies' writer Matt Charman is attached as lead scriptwriter for the adaptation.

Managing Director Damien Timmer, said: "This was one of those rare manuscripts which gave me goosebumps as I was reading it.

"An utterly immersive and riveting read, Maxwell Knight is a genuinely fascinating character, and his journey through some of the most turbulent years of the 20th century constantly astounded me. It's a real passion



Matt Charman

project for Matt Charman and Mammoth and we look forward to starting on it!"

He added: "It really has everything you'd want from a great espionage story: incredible agents risking their lives; the highest possible stakes, with the safety of the world hanging in the balance; and at its heart a complicated, mercurial spymaster spinning an ever more intricate web."



Speaking of his new position, Mr Fleming said: "It is a great privilege to be asked to lead GCHQ... from managing cyber risks posed by nation states to preventing terror attacks, keeping our children safe online and supporting our armed forces, the exceptional men and women of GCHQ operate on the new frontline of global challenges."



Sir Mark Grant

UK National Security Advisor Sir Mark Grant said of the appointment: "Jeremy is widely respected across the national security community."

Mr Fleming, Deputy Director of MI5 since 2013, takes control at a challenging time following spying allegations made by Donald Trump's Press Secretary, Sean Spicer. He claimed sources stated GCHQ, NSA's sister organisation, had helped President Barack Obama spy on the then presidential candidate. The allegations prompted an angry response from senior GCHQ officials, which in turn forced the White House to say "they will not be repeated." (See page 50) Mr Fleming will visit the United States later this summer.

Al-Qaida Number Two Killed

End Game for Senior AQ Terror Veteran

US intelligence officials have confirmed a Hellfire missile fired by a CIA-controlled UAV has killed senior al-Qaida operative Abu al-Khayr al-Masri. The 59-year-old Masri was in a vehicle when the attack took place in February near the northwestern city of Idlib, Syria.

Masri, a.k.a. Abdullah Muhab Rajab Abdulrahman (below), was al-Qaida's 'number two' and a close friend and associate of the group's leader, Ayman al-Zawahiri. Married to one of Osama bin-Laden's



daughters, he was also a member of the terror group's Shura Council.



The missile struck the roof of Masri's vehicle with deadly precision

Intelligence sources state Masri was directing operations in Syria, performed by Jabhat Fateh al-Sham, an al-Qaida franchise spawned from the al-Nusra Front.

The CIA had flagged Masri as a lead planner of the 1998 attacks on the US embassies in Kenya and Tanzania.



POISONED SOUP MYSTERY

A Key Investigative Question Never Asked

Alexander Perepilichny, 44, the Russian whistleblower who died while jogging near his Surrey, London home in 2012, may have been murdered by eating poisoned soup. His death was originally attributed to natural causes, but a subsequent investigation revealed that traces of a rare chemical, which can be found in the poisonous plant gelsemium elegans, had been found in his stomach.

Perepilichny, who had sought refuge in Britain in 2009, had been

providing evidence against individuals linked to the death of lawyer Sergei Magnitsky who was beaten to death in a Moscow jail in 2009. Magnitsky had accused Russian government officials of



Alexander Perepilichny

stealing \$230 million in a money-laundering scheme.

In November 2016, a court assigned PII - Public Interest Immunity status to the Perepilichny case. This effectively meant details would remain secret at an inquest on national security grounds. The original coroner has since been replaced and senior judge, Nicholas Hilliard, said the PII documents were not significant.

Details about the Perepilichny case remain shrouded in mystery and



few doubt his death has links to Moscow's intelligence underworld. Bizarrely, it has emerged his widow was not asked about what he had eaten the day he died. Perepilichny did in fact eat a Russian soup containing sorrel. Speculation abounds that poison may have been substituted. An inquest begins 5 June 2017.

ANOTHER DARK DAY IN LONDON

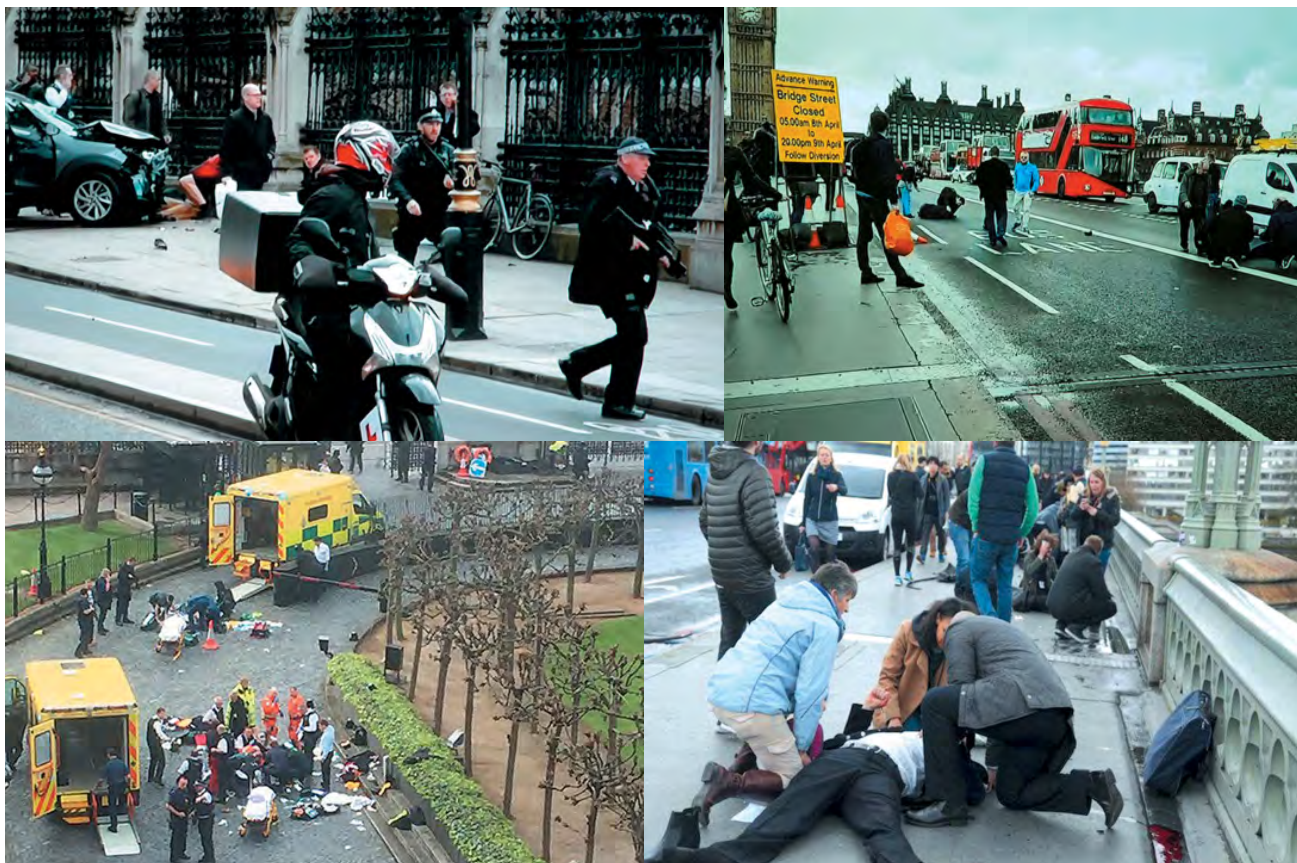
MI5 had lone wolf operative under surveillance for liaisons with ISIS supporter



Khalid Masood

82 SECONDS

ISIS-INSPIRED TERRORIST ATTACKS IN LONDON



'USE CARS AND TRUCKS AS WEAPONS'... ISIS INSTRUCTION 2016

Few city areas in the world are guarded like those in and around Whitehall, London. In the past decade new security measures, including external building concrete and steel security pillars, bomb-proof glass and an array of CCTV cameras have been installed. Combined with dozens of visible police, armed officers and covert surveillance watchers, plus a rather secret security element, those who work in or visit the tourist area, feel reassured. Yet despite all of this, and a terror level which has been fixed on Severe for some time, just

one man driving a car brought chaos to the city on 22 March in a rampage that lasted but 82 seconds.

Naturally ISIS claimed responsibility for the attack outside the British Parliament that left five dead, including one police officer, and 50 others injured; some critically. The incident, watched by millions of people around the world, took place on the first anniversary of the suicide bomb attacks at Brussels airport and underground system, killing 32 people.

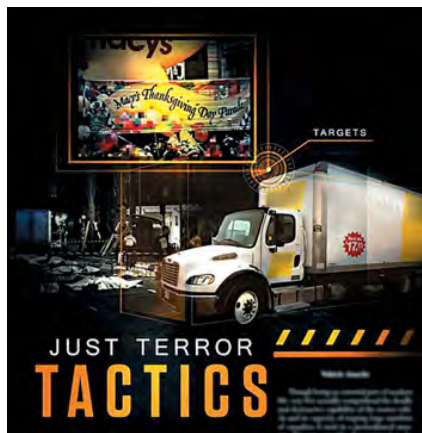
A SIMPLE ATTACK PLAN

The terrorist, identified as Khalid Masood from Birmingham, had travelled from Brighton to the capital. At 2.40pm he drove his rented Hyundai 4x4 at high speed over Westminster Bridge, mounted the pavement and struck dozens of pedestrians. It was all so very reminiscent of recent attacks in Nice, Berlin and Jerusalem.

Masood then crashed his SUV into iron railings outside the Palace of Westminster and ran towards a usually well-protected diplomatic and staff access area with two knives. Once inside the gates, he stabbed 15-year police veteran and father Keith Palmer, 48, multiple times before a diplomatic close protection officer shot him three times in the chest. Attempts were made to revive the officer, but failed. The attack, at the very heart

of Britain's seat of power, was over. Parliament offices were secured and Prime Minister Theresa May evacuated by car from the scene. Dozens of armed specialist counter-terrorism officers, including a number of SAS officers were mobilised and streets sealed off.

Just hours after the incident, UK officials announced Masood was known to police and MI5. ➤



ISIS magazine with vehicle attack feature. The article prompted major security alerts in New York and other cities around Thanksgiving Day



Anjem Choudary



Police officer Keith Palmer was unarmed at the time of the attack and had just ushered several people to safety. MI5 as yet, has found no direct links between Masood and ISIS, though are working on the assumption he had been inspired by the terror group's car attack rhetoric - and was opposed to UK military involvement in attacks on ISIS positions in the Middle East

© SNAPPERJACK OF LONDON

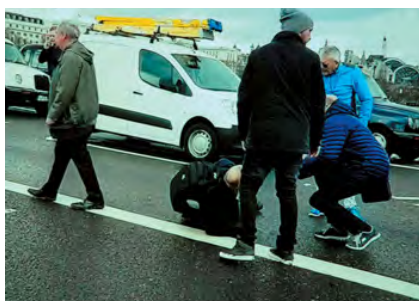


ISIS Internet warning for London prior to the attack by Masood

THE ATTACKER

Theresa May said in a statement: "He was a peripheral figure. The case is historic. He was not part of the current intelligence picture. There was no prior intelligence of his intent or of the plot."

Shortly after the attack, the British-born terrorist was referred to by an ISIS Internet writer as 'one of its soldiers'. However, the



general consensus amongst intelligence and security analysts is he had no direct or even loose connection with the terror group, nor was the operation controlled or assisted. A London police official told Eye Spy, "analysts indicate he was inspired not directed by ISIS." Despite this, and perhaps of relevance, it later transpired that moments before he attacked, Masood had used the encrypted messaging service WhatsApp. Police acknowledge they still do not know who he was in contact with. Home Secretary Amber Rudd said it was "totally unacceptable that the security services were shut out from messages of this kind." The Home Office is now exploring new legislation which could force social networking companies to provide information.

RAIDS ACROSS BRITAIN

MI5 and NSY launched various raids in Birmingham, London, Manchester and elsewhere, with much focus on Masood's flat in Birmingham. The vehicle used in the attack also had connections with the city - it had been rented from Enterprise in nearby Solihull

- eight miles away from his residence. Indeed, a sharp-eyed Enterprise worker recognised the registration number of the car hire vehicle on the bridge and contacted police immediately.

Masood's identity was known to several journalists long before NSY released his name. However, the media agreed not to publish his

Continued on page 74



Masood at school in Kent

NK OFFICE



Kim Jong-nam

225

ANALYSIS

North Korea Spy Agency Behind Assassination of President's Half-Brother Kim Jong-nam

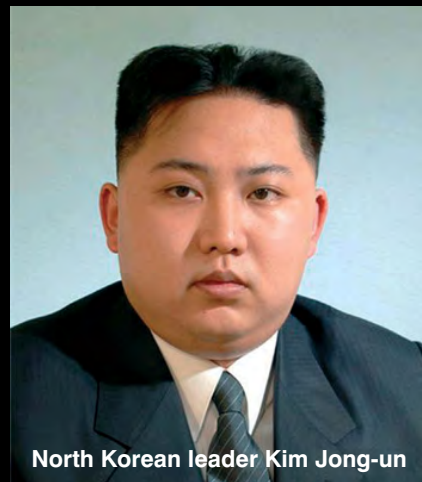
AN EXECUTIVE ORDER

Travelling under the assumed name of 'Kim Chol', Kim Jong-nam, 46, was the half-brother of North Korean leader Kim Jong-un. A former senior official in the Ministry of Public Security, he was once favourite to assume the leadership of his father, Kim Jong-il, who died in 2011. However, the crown prince suffered from various personal issues and several scandals conspired allowing his brother to take the reins. Viewed as a liberal, he had taken up residence in Macau, China, where he openly criticised Jong-un, describing him as a dictator. He also called for a reunification of the Koreans.

Jong-nam was murdered in an audacious poison attack inside Kuala Lumpur International Airport (KLIA2), Malaysia, on 13 February. Newswire reports initially said he had been attacked by two women using a syringe. However, armed with CCTV and various statements from the public, a very different attack scenario emerged. One eye witness said, "someone grabbed him from behind and splashed liquid on his face," whilst a second said "a cloth appeared soaked in a liquid." A second woman then sprayed an aerosol directly towards his face. The women

then raced to the toilet where a witness said they washed their hands. One woman was seen vomiting.

Jong-nam immediately sought assistance from airport workers at an information desk, before explaining to police what had happened. He was then taken to a washroom. However, he soon became unwell and an ambulance was called. He died enroute to Putrajaya Hospital - less than 20 minutes had expired. Before he passed, he explained he was "sprayed with liquid" and it was "very painful... very painful." The incident took place



North Korean leader Kim Jong-un

outside the passport checking office as he waited to board a flight to Macau, China.

Eye Spy sources believe he was killed by a spy network known as Office 225, operated by North Korea's primary intelligence agency - Reconnaissance General Bureau (RGB). This element is attached to one of six RGB bureaus



20 MINUTES FROM DEATH

1-2. Kim Jong-nam walks through airport terminal. 3. He stops to examine flight information. 4-5 Doan Thi Huong approaches him from behind and rubs cloth into his face. 6. Jong-nam explains what happened to airport security officials already stating he feels unwell. 7. He is taken to a rest area by police



Leading the investigation - Malaysia National Police Deputy Inspector-General Noor Rashid Ibrahim (left)

known as the clandestine service. It has been responsible for numerous underworld attacks over the years and uses long-embedded sleeper agents and others protected by diplomatic cover. The media have blamed several other secretive NK agencies.



General Khalid Abu Bakar

from the CCTV footage at the airport," said Inspector General Khalid Abu Bakar. Hours earlier a CCTV still frame of the woman was released by police. Asked if the arrested woman was the suspect in the image, a senior official said: "It is her. We believe she was involved in the

ARRESTS AND SUSPECTS

Security services in Malaysia studied CCTV footage inside and outside the airport, and soon identified two female persons of interest. For a time they were seen standing next to Jong-nam, before one is seen to attack him from behind, smothering his face with a cloth. Moments later she departs in a taxi. Forty-eight-hours later officials revealed a 28-year-old woman had been arrested in connection with the murder. "The suspect was positively identified

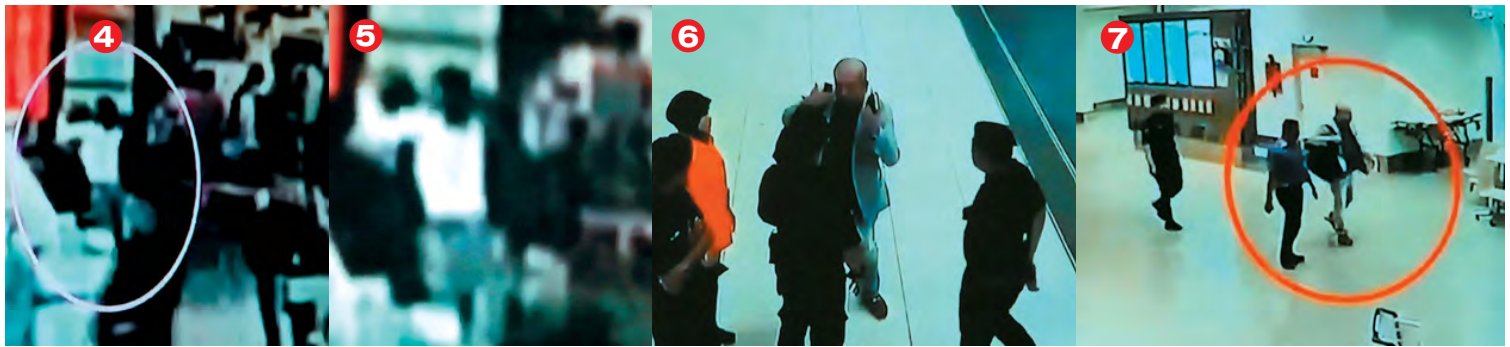


Kuala Lumpur International Airport (KLIA2), Malaysia

incident." The suspect was detained at the airport on 14 February as she tried to board a flight to Vietnam. She was carrying a Vietnamese passport and used the name Doan Thi Huong. The following day an Indonesian female named as Siti Aisyah, 25, and a Malaysian male named as Muhammad Farid Bin Jalauddin, 26 were detained in connection with the attack. Aisyah is believed to be the second woman captured on airport CCTV. A taxi driver was also arrested.



Kim Jong-nam pictured slumped in a chair shortly before he died



Siti Aisyah's passport detail



North Korean individuals: Ri Ji Hyon, 30, Hong Song Hac, 34, O. Jong Gil, 55 and Ri Jae Nam, 57. A few days later two more names were added to the wanted list - Kim Uk Il, 37 a worker for Air Koryo and Hyon Kwang Song, 44, second secretary at the North Korean Embassy (above left).

GAME FOR A LAUGH - A \$90 TELEVISION PRANK?

Intelligence officials from various nations have examined the case with interest. The attack was brazen and in a very public area. Similarly, the



Kim Jong-nam travelled widely and was a frequent user of social media. Some journalists have speculated this made him an easy target to track

On 18 February police said they had arrested a fourth person in connection with the case - a 46-year-old man from North Korea. He was later named as Ri Jong Chol, a chemistry scientist who studied in Pyongyang. At the

same time, CCTV images of four other men were released - all of whom are suspected of playing a role in organising Jang-nam's murder. The suspects departed Malaysia just hours after the assassination, and police believe they are members of North Korea's main intelligence agency - Reconnaissance General Bureau. In a press briefing Deputy Inspector-General of Police Noor Rashid Ibrahim released the names of the



Doan Thi Huong



Siti Aisyah



Ri Jong Chol



Muhammad Farid Bin Jalauddin

assassins will have been fully aware of CCTV. Officials were puzzled with a statement made by Huong. She told police she had been tricked into playing a television prank on Jong-nam, and thought it was "harmless fun." Her male associates had promised her a fee of \$90 to perform the act. Huong's explanation was rejected by investigators, but some intelligence watchers believe the story, whilst outlandish, might just be true. Malaysian police said the women were "the lizard's tail," a description thought to mean hired, expandable assets. Deputy Inspector-General Ibrahim said "they knew exactly what they were doing." The *China Press* said both women knew each other and had previously worked in China as female escorts.

North Korean officials made a desperate bid to halt Malaysian forensic specialists performing an autopsy on the body of Kim Jong-nam, demanding that it should be returned post-haste to Pyongyang. This was rejected. "If North Korea was behind the attack," said South Korea's Prime Minister Hwang Kyo-ahn, "then it would clearly depict the brutality and inhumanity of the Kim Jung-un regime." An initial autopsy proved inconclusive, but officials still insisted he was poisoned, including South Korea's National Intelligence Service (NIS) Director Lee Byung Ho. "Poison was used," he said.



South Korea's National Intelligence Service (NIS) Director Lee Byung Ho

On 24 February, Malaysian officials released a toxicology report that revealed traces of a VX nerve agent had been discovered in Jong-nam's eyes and mouth. Designated a weapon of mass destruction by the United Nations, VX is almost always fatal if ingested, inhaled or



**Most wanted. Almost certainly engaged in the Office 225 operation - three suspects who returned to North Korea just hours after the assassination.
L-R: Ri Jae Nam, Hong Song Hac and Ri Ji Hyon**



Doan Thi Huong caught on camera at Kuala Lumpur International Airport

comes into contact with the skin and absorbed. Initial symptoms include pain, blurred vision, drowsiness and vomiting. It can take on the form of a spray, vapour or liquid. For its part, North Korea said because Doan Thi Huong was not wearing any protective gloves when she smeared the cloth over Jong-nam's face, this proves that a deadly toxin was not applied. However, security officials who watched her movements on CCTV after the attack, noted her rush to the washroom - indicating she was fully aware that she should wash her hands immediately.

Malaysia withdrew its ambassador to North Korea and summoned Kang Chol, Pyongyang's ambassador to "seek an

explanation" on accusations that the country was "trying to conceal something in connection with the autopsy."



Checkpoint at the Korean Demilitarised Zone (DNZ) separating North and South Korea

A HISTORY OF ASSASSINATION

NORTH KOREA'S DEADLY AGENT RUNNERS

North Korea has a long tradition of using agents and proxies to carry out assassinations. Its secretive spy agency has been compared to the Mossad. MI6 is but one organisation aware of several incidents linked to NK assassins, and most involve the use of poisons. In previous cases, victims, including defectors, opponents and human rights' activists have been jabbed by poison-filled syringes or pens. Some of these 'delivery' items have been secured by South Korea's NIS and contained deadly toxins. One of which can kill in around three seconds.

CASE EXAMPLES

In August 2011, South Korean pastor, Patrick Kim, was killed near the China-North Korean border. He was found collapsed and foaming from his mouth. National Intelligence Service officials said the activist, who had engaged in secret operations to help people escape North Korea, was almost certainly assassinated using a poison injected by a syringe. A day later another anti-NK activist in the Chinese city of Yanji was attacked by a needle-carrying assassin - he survived. A former NIS officer said, "the poison needle has been in use by North Korean special operations for a long time."

Weeks later in September, an attempt to kill well known activist Park Sang Hak occurred. Hak, a member of the Fighters for a Free North Korea (FFNK), had enraged Kim Jong-il by sending bin bags attached to helium balloons containing anti-NK literature, dollar bills, DVDs and miniature tunable AM/FM radios. The

balloons travelled over 100 miles even reaching the capital Pyongyang. Messages read '*Kim Jong Il is lying to you*'. The radios also allowed North Koreans to tune into Free North Korea Radio and listen to propaganda from the south.

An Office 225 agent known only as Ahn, befriended Hak and had arranged to meet him outside a subway station in Seoul. However, NIS officers lay in wait and arrested him before the encounter took place. Ahn had been instructed to kill Hak, who was designated 'Enemy Zero' by the RGB. Ahn was carrying various items, including a pen containing neostigmine bromide, two guns that delivered poison and various poison pills.



Defectors too have revealed intimate details of kill operations. One such person, Kim Hyon-hui, explained how she was groomed by the country's Reconnaissance General Bureau and planted a bomb on a South Korean airliner in 1987. Korean Air Flight 858 was flying from



Kim Hyon-hui planted a bomb on Korean Air Flight 858 in 1987



RGB agent Kim Hyon-hui

Baghdad to Seoul when the device exploded killing all 115 on board. The incident led to widespread sanctions and the United States designating North Korea as a state sponsor of terrorism. And the list of abduction cases and missing persons is lengthy. ➔



An Office 225 agent was instructed to kill Park Sang Hak of the Fighters for a Free North Korea



Poison-delivering items used by agents of North Korea's Reconnaissance General Bureau (RGB)

"the poison needle has been in use by North Korean special operations for a long time..."

AGENT COMMUNICATION FOR YOUR EYES AND EARS ONLY

By Paul Beaumont

Following the assassination of Kim Jong-nam, Eye Spy focussed on the secret manner in which North Korea communicates with its overseas outposts and agents. One such method is virtually impenetrable to would-be listeners, and relies on Number Stations and an old piece of spy tradecraft - the One-Time Pad.

Number stations send messages to spies working overseas on behalf of a nation. Russia is the sender of most clandestine messages today; during the Cold War the countries involved with such transmissions included the USA, USSR, East and West Germany, Great Britain, France, Israel, Czechoslovakia and a host of other Iron Curtain Countries. Communications need to be covert and secure; one way of achieving this is using radio, usually via short wave or sometimes medium wave stations.

The transmitted message itself will be sent using either Morse, Voice, Polytones, Data pulses or as a Hybrid consisting of a mixture of Voice or Morse with Data.

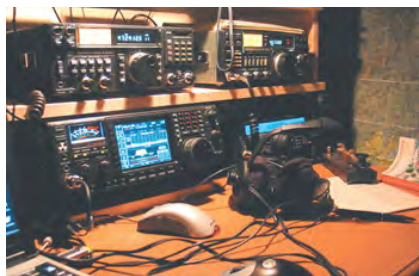
Decoding Voice or Morse is achieved using a One-Time-Pad which contains pages of groups of numbers. When applied to the message - text reveals the wording or instruction.

ANALYSIS OF A MESSAGE

Such a message may look like this actual five group message sent by North Korea on 23 February 2017: [674] [213] [5] [33362] [32079] [40063] [40372] [89762] [213] [5] [00000] (Brackets added by Eye Spy).

Readers will note 11 number groups, six are administration. 674 is likely the agent identity, 213 the decode key and 5 the group count. 00000 informs the recipient message has ended.

Number stations usually make an announcement to indicate a transmission; in the case of the



example message a voice would announce 674 674 674 for two minutes, others have used a sounding gong, pop music and two tones.

North Korean Intelligence sent a message using the external service of Radio Pyongyang (Voice of Korea) at 1615GMT on 15 September, 2016. The programming broke with a song: 'We will go together with a song of joy' [indication of transmission]. Followed by an announcement: 'We will notice the repetition homework of the science of Distance Learning University for number 27 exploration agency' [the agent ident and group count].

It is possible the 15 September message, repeated later on 29 September, are linked to the planning stage in the assassination of Kim Jong-nam. In this case alerting agents of his movements across the Far East.

• Paul Beaumont has written an in-depth report on the mechanism of the North Korean messages - see www.eyespyimag.com - Spy Byte of the Month or Eye Spy's Facebook page



North Korean Number 6202 Table (decode grid) - and digital shortwave receiver



Former leader Kim Jong-il

As for Jong-un, intelligence sources state he deliberately used various names to cover his movements. Indeed, police believe he has been under threat of assassination for at least five years. Kim Yong-su, an intelligence agent from North Korea was jailed in South Korea in 2012, after admitting he had been despatched to organise a hit-and-run car attack on Jong-un - just one of a number of known operations which failed.



Kim Yo-jung

Much speculation still exists why he was targeted, given his reluctance to seek office in North Korea. However, other intelligence analysts and specialists believe



Most wanted. Clockwise from top left: Ri Ji U, Hong Song Hac, Kim Uk Il and Ri Ji Hyon



Face of an assassin? Doan Thi Huong

the plot may have been orchestrated by Kim Yo-jung, the younger sister of the current NK leader. She is vice director of a rather secretive unit known in the West as the Propaganda and Agitation Department (PAD). The PAD helps

promote Kim Jong-un's image in North Korea and around the world. Others, however, blame the RGB. Cheong Seong-chang, of the Sejong Institute said: "This agency has been spying on him and they are in charge of assassinating dissenting officials."

Kim Jong-un has a global reputation for eliminating opponents, including members of his own family. In 2013 he ordered the execution of his uncle, Jang Sung-taek, who was a powerful figure in North Korea and Vice Chairman of the National Defence Commission. He was accused of being a counter-revolutionary. Reports also emerged of various executions of other family members.

Whilst sources in Malaysia are confident two females carried out the assassination, police believe at least ten men played a part in the operation.



Kim Jong-un ordered the execution of his uncle, Jang Sung-taek in 2013

NORTH KOREA'S WATCHERS

Whilst Office 225 is the likely director of the assassins via the Reconnaissance General Bureau (RGB), various shadowy NK directorates exist



Leader Kim Jong-un and senior government and political operators are shielded by the **GUARD COMMAND (GC)**, an organisation with close ties to the armed forces and Reconnaissance General Bureau (RGB). Intelligence sources in the West believe the GC has access to chemical weapons.

The **STATE SECURITY DEPARTMENT (SSD)** or Ministry of State Security, is a country-wide organisation charged with ensuring civil order, and identifying possible subversives, spies or defectors. It has been described as a counter-intelligence agency.

Another agency linked to intelligence is the so-called **THIRD FLOOR**. Whilst its activities are not fully understood, the organisation operates in the business world, and is a general collector of intelligence. Third Floor operations are widely

conducted overseas and some of its officials have direct ties to the country's leadership. It takes its name from the building floor level of the Workers Party of Korea Central Committee in Pyongyang.

ROOM 39

Following the assassination of Kim Jong-nam, Indonesia National Police have announced they will investigate what they believe is a North Korean spy network operating from a restaurant in Jakarta.

According to intelligence reports, North Korea's RGB has been operating in Malaysia, Singapore and Indonesia using spies with cover careers as engineers, technical consultants in the construction industry and restaurant operators.

"They use the restaurants as a main front to conduct intelligence gathering and surveillance, targeting Japanese and South Korean politicians, diplomats, top corporate figures and businessmen who visited or were based in these countries," a source in Indonesian intelligence said. "There is also an apartment located above a North Korean restaurant in Jakarta that is part of the RGB Indonesia office."

Although the National Police have not named the restaurant, it is widely reported that the establishment is **PYONGYANG**, part of a chain of 130 restaurants named after the capital of North Korea and based in a dozen countries around the world. They are owned and operated by the Haedanghwa Group, an organisation of the government of North Korea.

According to reports, the restaurants are one of several overseas business ventures of **ROOM 39**, a North Korean government organisation dedicated to acquiring and laundering foreign currency for the North Korean leadership.

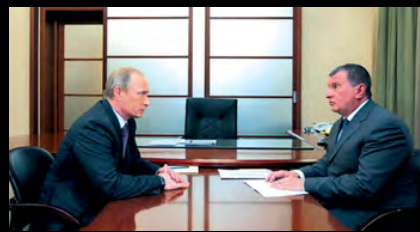
North Korean defectors report that the restaurants are run by local middlemen who are required to pay between \$10,000 and \$30,000



each year to the North Korean government; are required to live on the restaurant premises and are closely watched by on-site North Korean security agents. According to reports, in the 2000s several attempted escapes by waitresses in China led to the closure of restaurants and the repatriation of their staff. In 2016, South Korea announced that 13 restaurant workers had defected from the Pyongyang restaurant chain abroad.



PAYBACK



In Eye Spy 107, we reported upon the unexplained death of Oleg Erovinkin, a former KGB general and chief of staff to Igor Sechin, the head of Rosneft, the country's huge state-owned oil company. Erovinkin was found dead in his car on 26 December 2016 in central Moscow. Several media houses have now attempted to link Erovinkin's death with former MI6 officer Christopher Steele's Trump dossier. This is in the context that he provided information to Steele concerning Rosneft, Sechin, secret deals, sanctions and a number of opportunities for Trump associates and Moscow.

Sechin was both a close friend and advisor to President Vladimir Putin. Indeed, Putin himself appointed Sechin as head of Rosneft some 10 years ago. There are stories and lines in the dossier that suggest a deal was being

brokered that would see US sanctions lifted on Russia if Donald Trump became President. Some commentators and intelligence watchers believe the secret liaisons and promises found their way to Steele via Erovinkin. All of this is hearsay, but Sechin was referenced several times by Steele, who did not name the primary source in connection with this part of the dossier. However, one line suggests Steele's source was close to Sechin. *'A trusted compatriot and close associate'*, wrote Steele. And here lies the connection.

The US media has published various stories concerning Russian contact with Carter Page,

described as an early Trump foreign policy advisor who visited Moscow in July and December 2016. Page, a former US military intelligence officer (US Navy), was familiar with happenings in Russia and had worked as an investment banker in the country. Here he advised companies on the best methods to do business. During Page's summer trip, he delivered a speech to graduating students at the New Economic



One source of the 'Trump dossier'? Oleg Erovinkin - still no official explanation of his death



Rosneft headquarters, Moscow

Hacking, Trump dossier, election interference, deaths, treason, arrests and intelligence agent contact combine to create...

A Dark Conspiracy



Carter Page - once described as a 'Trump Advisor' at the New Economic School

"Carter Page is an individual whom the president-elect does not know and was put on notice months ago by the campaign..."



Sean Spicer

School in Moscow. And it was at this time, Steele's unverified, unsupported and raw intelligence dossier says that various offers were made by Russia, including a stake in Rosneft. There are further claims Sechin met with Page.

In December last year, Page denied being a Trump advisor and dismissed suggestions he had attempted to create a back-channel for Trump and the Kremlin. A Kremlin official also rebuffed suggestions of a liaison.

In January, when the Trump dossier emerged, White House Press Secretary Sean Spicer said: "Carter Page is an individual whom the president-elect does not know and was put on notice months ago by the campaign."

White House Press Secretary Sean Spicer

MARCH 2017

The Senate Intelligence Committee is looking into claims of improper contact with Russian officials during the United States General Election campaign. As part of its endeavour, the committee wrote to various people asking that they 'preserve materials that may be relevant to the investigation'. One of those who received the letter was Carter Page. Mr Page's response was: 'I am writing to ➤

BACK TO THE DAY JOB

No Comment From Former MI6 Man



Former MI6 officer Christopher Steele, the compiler and author of the Trump 'dirty dossier,' has returned to work after disappearing for almost two months. Steele, gave a brief statement outside the offices of his Belgravia, London intelligence firm, Orbis. "I'm now going to be focusing my efforts on supporting the broader interests of our company here. I'm really pleased to be back here working again at the Orbis's offices. I'd like to say a warm thank you to everyone who sent me kind messages and support over the last few weeks. Just to add, I won't be making any further statements or comments at this time."

The creation and subsequent release of Steele's report allegedly caused dismay at MI6. It is not known if the Service questioned him regarding its content, though some intelligence watchers believe this was an inevitable consequence.



FSB headquarters, Moscow



President Putin with Rosneft chief Igor Sechin

let you know that I have received your letter and will be more than happy to provide any information which may be of assistance to the committee. In the meantime, I will do everything in my power to reasonably ensure that all information concerning my activities related to Russia last year is preserved’.

For the record, the FBI has also launched a separate and autonomous investigation into alleged Russian interference in the election. And Page has inferred his cell phone may have been tapped.

As for Erovinkin, a Russian security analyst and intelligence watcher told Eye Spy: “He was different... he was a link man who gave away stories and these found their way to Steele. I don’t know if they are accurate, but they infuriated Putin and other Kremlin

officials. Sechin was a friend of Putin, and is a very powerful man. That Putin supposedly made a deal with Trump, would be a serious matter - and Erovinkin - had he not died, would have been arrested and questioned by the FSB anyway.”

Erovinkin, 61 was found slumped in his car. His body was taken away by emergency services under the watchful eye of an FSB team. Russian news agency RIA Novosti, said the spy service was dealing with his autopsy. To date, no official reason has been given for his death, but speculation is rife in the Russian media. Several informed editors and commentators believe he died as a result of foul play. Sources have confirmed there were no obvious injuries to his body leading to much speculation he died of a heart attack or something more sinister - poison.

INTEL QUESTIONS



In the USA, moves are afoot which could see Christopher Steele interviewed by senior American political officials on neutral territory. This coincides with reports Steele would be unwilling to give evidence in the USA.

It is already known Steele had contact with the FBI, but members of the House Intelligence Committee are keen to hear testimony from the author of the Trump dossier directly.

Republican Adam Schiff said: “If there’s an issue about whether he is willing to come before the committee, I can say I am more than willing to go to him, and I know there are other members of the committee would join me in that.”

Questions would be raised about sources, sponsorship and ultimately, the objective of the dossier. His pre-dossier release liaisons with the FBI may also be discussed.

DETENTIONS AND SUSPICION

RUSSIAN INTEL MEN ACCUSED OF CIA CONTACT

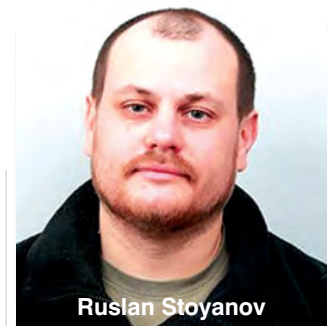
In January, two Russian FSB intelligence officers employed in cyber security and a prominent civilian cyber figure were arrested. The FSB officers were charged with treason - passing ‘[state secrets] to US interests’. The men were identified as Sergei Mikhailov and Dmitry Dokuchayev, both

of whom worked at the FSB’s Information Security Centre. The third man was named as Ruslan Stoyanov, head of Kaspersky’s computer incidents investigation team. The arrests appear linked to interference in the United States General Election campaign, Russian newspaper *Kommersant* reported.

An Interfax source referenced the CIA. “Sergei Mikhailov and Dmitry Dokuchayev are accused of betraying their oath and working with the CIA.” For a media platform like Interfax to make such a claim must have been green-lighted by the Kremlin. However, it does not necessarily mean the accusation is true. Dokuchayev, is alleged to be a former cyber hacker who used the name ‘Forb’. He supposedly agreed to work for the FSB to avoid jail.

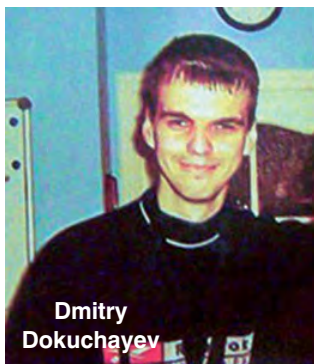
Other Russian journalists believe the charges against Stoyanov relate to a period before he joined the company in 2012.

Former CIA officer Steven Hall, a Russian Desk specialist



described the arrests as more than relevant. “They may be just the tipping point concerning Russian hacking.” Moscow sources, however, are satisfied the arrests were made in connection with hacking commentary which appeared in Christopher Steele’s Trump dossier.

Internet news website Life, with supposed links to Russian Intelligence, alleged when the FSB searched Dokuchayev’s residences, they found paper money in various hideaways amounting to £10 million.



LANGLEY'S NOT SO SECRET

'we will drop a bombshell that will blow the world away in 2017'

start.. wikileaks:showtime...

VAULT 7

CIA branches named as WikiLeaks release batch of files identifying popular gadgets and electronic media targeted by Langley's cyber spyware elements

A few months ago WikiLeaks promised to 'drop a bombshell that would blow the world away in 2017'. It also warned that a showdown with the intelligence community was coming. The rhetoric was a precursor to a release of newly secured intelligence files, this time detailing many secrets CIA related to Langley's surveillance and electronic arms - one such being the Embedded Devices Branch (EDB), which falls under Center for Cyber Intelligence (CCI). The last significant release of documents was of course, e-mails hacked from the account of Hillary Clinton's 2016 General Election manager John Podesta. Also referenced under

a header of 'Fine Dining' is the CIA's Operational Support Branch (OSB). This Directorate or Mission is a known support element where different tasks are examined and support provided. In the case of Vault 7, the OSB is described as an interface where technical staff examine various electronic items suitable for use in operations. Numerous other elements are also identified.

The release of new CIA documents, collectively codenamed Vault 7, comes at a particularly sensitive time, and amidst disputed claims of hacking, wiretapping, surveillance and eavesdropping at Trump Tower. Running parallel to the Trump Tower



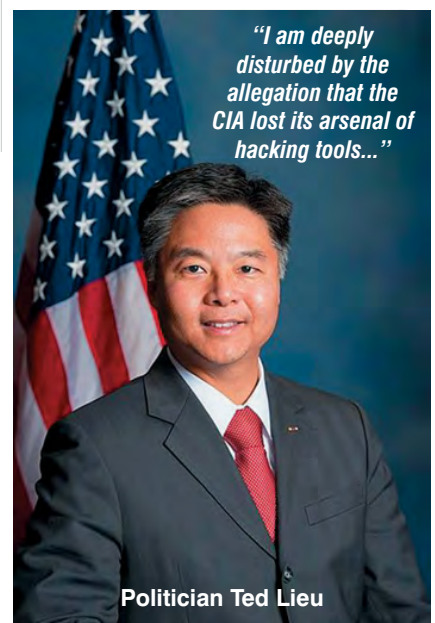
debacle, the Senate Intelligence Committee and FBI are involved with investigating Russian cyber interference in the race for the White House.

Few would argue with WikiLeaks claim that the release of the Vault 7 material represents the biggest exposure of sensitive US Intelligence files in history (number of documents in a single breach). The website boasted: 'The quantity of published pages in Vault 7 part one (Year Zero) already eclipses the total number of pages published over the first three years of the Edward Snowden NSA leaks'.

It's not known of course, just how many documents are in the file, but analysis ➤



CIA headquarters, Langley



Politician Ted Lieu



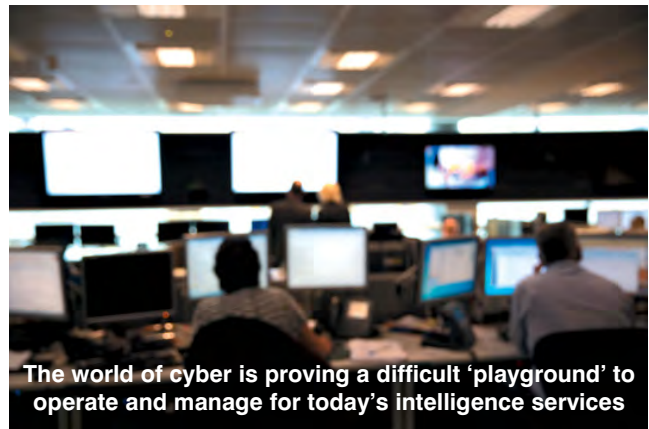
Vault 7 documents expose the CIA's interest in 'engineering' everyday electronic devices into tools capable of assisting investigations



seems to suggest the first release - 'Year Zero' - is but part of a sequence. WikiLeaks reported: 'Year Zero, comprises 8,761 documents through 2016 and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virginia'.

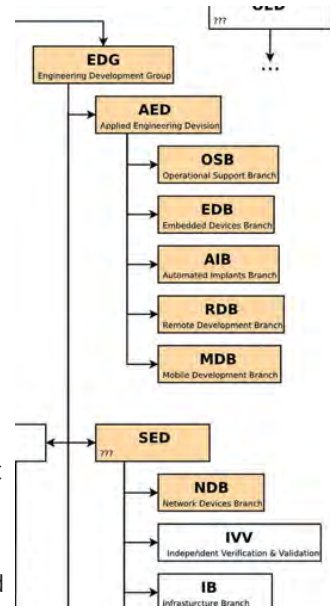
YEAR ONE: ANALYSIS OF VAULT 7 FILES

'Year Zero' exposes the wide range of targeted operations, some insight into its direction, and interestingly, alleged liaison and actual cooperation with British Intelligence on a programme codenamed Weeping Angel. This is essentially an EDB endeavour which focuses on turning everyday items into surveillance devices. However, far from WikiLeaks claim that this is 'new and revealing', such programmes have been in existence for decades, and the CIA are but one of dozens of intelligence services engaged in this type of work - or spyware. What is damaging



The world of cyber is proving a difficult 'playground' to operate and manage for today's intelligence services

and somewhat embarrassing for Langley, is that the documents reference targeted products. These include Samsung F8000 televisions, Apple's very popular iPhone, Google's Android and Microsoft's Windows - all day-to-day objects used by millions to communicate. WikiLeaks also referenced another CIA research element called the Mobile Devices Branch (MDB). This team specialises in remotely hacking and controlling popular smart phones. Malware is uploaded in a technique called 'Persistence' in the Vault 7 material. It remains put even when the cell is switched off and on. The hack bypasses all encryption and defence barriers allowing access to all material and conversations. Even a decade ago, receipt of a simple text message left such devices vulnerable. A further programme showed Langley was working on ways to engage with the electronic control system of vehicles.



Some of the CIA branches allegedly caught up the security breach

The art of turning cell phones into working 'spy phones' has been around for two decades. "If it's connected to the Internet or communicates with other systems - it can be accessed," a former CIA intelligence technical operator told Eye Spy.



The hacking of Hillary Clinton's General Election manager John Podesta (inset) seems an eternity ago as new case files relevant to cyber security and hacking surface almost daily

Internal investigators at Langley and the FBI have launched an investigation to identify the person or persons responsible for securing the files and passing them to WikiLeaks. Much speculation is directed towards Russian hacking outfits and interestingly, US Government contractors. However, until evidence is secured, this aspect will never be fully known - but it is a worry for the CIA and organisations such as NSA. Dates on the papers suggest the breach occurred in early 2016.

PURPOSE OF THE LEAKS?

Asked directly by the media how the website obtained the files and the purpose of publication, WikiLeaks said: *'The source wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons. Once a single cyber weapon is loose it can spread around the world in seconds, to be used by rival states, cyber mafia and teenage hackers alike'.* Undoubtedly an attempt to sound patriotic.

Naturally, those suspicious of domestic spying by the CIA, were vocal in their disapproval,



Sean Spicer

whilst others said the loss of such technology to third parties left the United States vulnerable. Democratic Representa-

WHAT'S A NAME?

WEeping ANGEL, MARGARITAS AND MOVIES

According to the leaked CIA documents, MI5's technical branch helped develop a piece of spyware (software) for Samsung's F8000 smart television sets codenamed Weeping Angel. In this case, the technology allows operators to listen-in to conversations of people close to the television - even when the set is turned off.



It is a name familiar to 'Dr Who' enthusiasts, and references a predatory monster which turns to stone when watched by others. However, it attacks when they close their eyes or turn their backs.

Weeping Angels first appeared in an episode of Dr Who in 2007 called 'Blink'. Dubbed 'The Lonely Assassins', Weeping Angels are described in sci-fi language as: *'Quantum-locked alien*



COURTESY: BBC

Weeping Angel from 'Dr Who'



Margarita

killers capable of hurling their victims back in time - allowing the Angel to feast on the energy of their un-lived days'.

Other hacking tools in Vault 7 are named after popular drinks and brands such as the cocktail Margarita and Wild Turkey bourbon; characters from movies such as Talladega Nights also appear.

tive Ted Lieu was one such person. He immediately called for an official investigation. "I am deeply disturbed by the allegation that the CIA lost its arsenal of hacking tools. The ramifications could be devastating. I am calling for an immediate congressional investigation. We need to know if the CIA lost control of its hacking tools, who may have those tools, and how do we now protect the privacy of Americans," said Lieu. White House

Press Secretary Sean Spicer said, "the leak was something everybody should be outraged about in this country."

Perhaps more concerning to the CIA, is a 'tweet' from WikiLeaks dated 8 March. *'WikiLeaks has released less than 1% of its #Vault7 series in its part one publication yesterday'.*

CIA STATEMENT ON CLAIMS BY WIKILEAKS

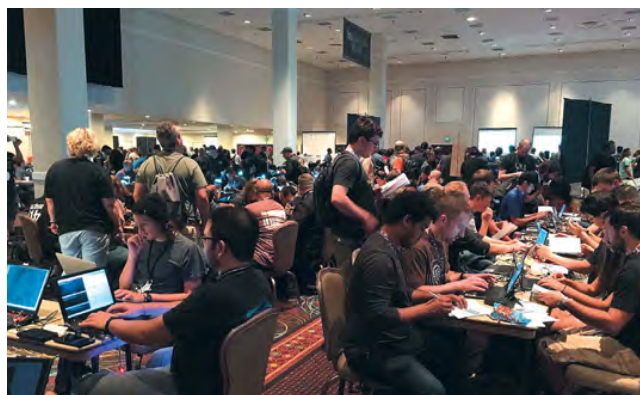


LANGLEY: We have no comment on the authenticity of purported intelligence documents released by WikiLeaks or on the status of any investigation into the source of the documents. However, there are several critical points we would like to make.

CIA's mission is to aggressively collect foreign intelligence overseas to protect America from terrorists, hostile nation states and other

adversaries. It is CIA's job to be innovative, cutting-edge, and the first line of defence in protecting this country from enemies abroad. America deserves nothing less.

It is also important to note that CIA is legally prohibited from conducting electronic surveillance targeting individuals here at home, including our fellow Americans, and CIA does not do so. CIA's activities are subject to rigorous over-



The CIA, FBI and Homeland Security are still uncertain if the material was hacked or 'presented' by an internal source to WikiLeaks

sight to ensure that they comply fully with US law and the Constitution.

The American public should be deeply troubled by any WikiLeaks disclosure designed to damage the Intelligence

Community's ability to protect America against terrorists and other adversaries. Such disclosures not only jeopardise US personnel and operations, but also equip our adversaries with tools and information to do us harm.

A TRAJECTORY TO LASTING DEFEAT

ISIS LEADER ADMITS DEFEAT IN MOSUL

Iraq media outlet Sumeria News has reported ISIS leader Abu Bakr al-Baghdadi, has ordered his followers in Mosul to hide and flee to the mountainous areas of Nineveh province. A purported letter from Baghdadi was circulated amongst his supporters, and follows fierce fighting between ISIS and Iraqi forces. The terror chief's departure from the former ISIS stronghold has been confirmed by the Pentagon.

Spokesman for Iraqi joint operations, Brigadier General Yahya Rasoul, said that the government has not yet confirmed the authenticity of Baghdadi's letter. "The Iraqi intelligence services are still monitoring the movements of Abu Bakr al-Baghdadi. If we discover Baghdadi's whereabouts, we will take immediate actions to arrest or eliminate him."

Described as a 'farewell speech', Baghdadi's note urged supporters to 'run and hide' or 'return home and blow themselves up with the promise of 72 women in heaven'.

US military monitors are uncertain as to the exact whereabouts of Baghdadi. In recent months a plethora of reports have surfaced regarding his health; some claim he had been

killed or seriously injured. One such report emerged following air strikes in Al-Ba'aj. His last public appearance was in July 2014, when he declared the creation of a caliphate. ISIS as an organised military fighting force, has been severely impacted by recent attacks by both Iraq and Syrian forces. One intelli-



Youngsters watch a building burn in the suburbs of Mosul

gence estimate said 30,000 terrorists have been killed, injured or fled since the beginning of 2016. In 12 months, the terror group has lost 65% of territory in the region. Another report, believed to have been compiled by the Pentagon, estimates 4,000 ISIS fighters remain in the Syrian city of Raqqa. "Despite a long road ahead for the US-led coalition in its fight to counter ISIS, the enemy is being degraded by every measure and is on a trajectory to lasting defeat," a Pentagon official said.



A US missile is readied for an air operation targeting ISIS terrorists in and around Mosul



Abu Bakr al-Baghdadi - terror leader unwell, injured or dead?

CHEMICAL WEAPONS WARNING

Britain's Minister of State Security, Ben Wallace, has entered the debate concerning the possible use of chemical weapons in the West by ISIS. "They [ISIS] have no moral objection to using chemical weapons against populations, if they could, they would in this country," said Wallace. He noted the terror group's desire for mass casualties.

British Intelligence has provided background on WMD and ISIS, referencing known dumps of such materials secured from various Syrian Government sites. Similarly, a number of casualties treated at

hospitals have unique injuries consistent with mustard gas usage.

- The Organisation for the Prohibition of Chemical Weapons (OPCW), has confirmed several WMD deaths.



UK Security Minister Ben Wallace



ENTRAPMENT & COMPROMISE

"For five years we bugged and burgled our way across London at the State's behest, whilst pompous bowler-hatted civil servants in Whitehall pretended to look the other way..."

Peter Wright MI5

History is littered with case files of people whose actions and words, historical, present and often unintentional, have come back to haunt them. Entrapment is a multi-faceted intelligence tradecraft used in numerous situations, from toppling presidents to recruiting spies...

There are a multitude of methods which can be used to entrap a target. And in the world of intelligence, hundreds of reasons why such an endeavour might be actioned. From exerting pressure to spy for an adversary; simple blackmail for financial gain or help broker arms deals, the reasons why entrapment is such a powerful tool are plentiful. Some operations are more complex, as recently evidenced in the US presidential election. Here



an attempt to 'pool' a plethora of unsavoury information and scandal was intended to derail a major political campaign. This was 'arms length'

entrapment - the information being so powerful, aggressive and embarrassing, it would leave Donald Trump with no where to hide and only one option - to halt his campaign. At the very least, the document was intended to impact upon the morale compass of the American people. However, besides a lack of referencing, a primary problem for those actors behind the report, and its author, former MI6 officer Christopher Steele, was time. Without proper supporting evidence, nothing could be proven. Part of the report focused on Mr Trump's alleged behaviour and liaisons before the election - two key elements in entrapment. Nevertheless, it was an audacious attempt to target one of the world's most powerful business figures.

ENTRAPMENT WITH AN EXIT DOOR

That the so-called Trump Dossier is stuck together by some stories sourced from the intelligence world is evident when one digests its sections. And the fact that it drew





INTEL INSIDE

Former US Secretary of State John Kerry with his entourage. Such high profile diplomatic positions invariably involve a great deal of travel to foreign locations, where attempts no doubt, take place to secure information on US intentions. His team must also behave impeccably, thus lessening the chance of entrapment or compromise

comment from various services, including MI6 (via the Foreign Office) and the FSB, only expose further, that entrapment methods are tools used by those whose task it is to recruit people in positions to augment operations and secure information. Let's not kid ourselves into believing entrapment is a no-go area for today's intelligence officials. In more recent times, the FBI have been accused of inventing terrorists and gun runners using entrapment in several high profile counter-terrorism operations. Few in the intelligence industry would disagree that exposing dangerous individuals intent on killing is wrong. Import-

tantly, whilst such operations progress, the Bureau includes and provides gateways allowing the individual[s] at various stages, an option to back-down or walk away. Indeed, FBI 'entrapment' in such cases has never been proven, despite those who sought to legally challenge underworld operators and the FBI's 'dark players'.

ESPIONAGE AND BLACKMAIL

In the theatre of espionage, securing the services of foreign agents and people who work in a variety of areas, from technology to



John Profumo, British Secretary of State. His activities and associations with spies, women and underworld characters left him open to blackmail

government, is an art which can involve entrapment. Sometimes an agent recruiter will be lucky, and a simple financial reward or the promise of a better life may prove pivotal. But in most cases, a great deal of background work will be necessary to discover if the person is suitable or susceptible to persuasion.

Quite often entrapment operations are enabled following a chance piece of information falling on the desk of a counter-intelligence officer, or a throwaway comment being made in a bar, for example. Indeed, this was the case in the mid-1960s, when MI5 embarked on a secret operation to recruit a senior KGB officer in the person of Sergei Grigovin (pseudonym).

The Security Service was fully aware that the KGB had laid down strict rules for Soviet diplomats and its own officers in respect of sexual liaisons with women whilst posted abroad. Moscow was still suffering from the ripples of the so-called Profumo Affair in the early 1960s, when Soviet naval attaché Yevgeny Ivanov became entangled in a spy affair involving various women, spies and the British Secretary of State John Profumo. However, when MI5 was made aware that a senior executive of Britain's *Daily Mirror* newspaper had learned that Grigovin was having an affair with a woman, it proved too good an opportunity to ignore, especially as there was a good chance of entrapment leading to possible recruitment.

And the chances of turning Grigovin improved when his affair with the unidentified woman ended, thus MI5 used its cunning to introduce the Russian to one of its undercover female agents. And whilst this liaison was developing,



FBI briefing



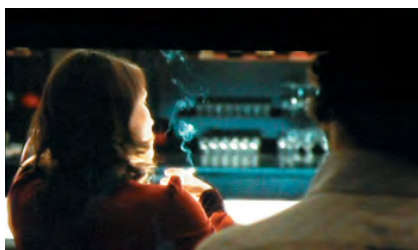
© THE INSIDER'S GUIDE TO 500 SPY SITES IN LONDON

Above left: Claridges Hotel, London. Used by world leaders, senior politicians, royal families and wealthy business people and celebrities. The hotel also became a target for MI5 listeners who installed listening devices in many 'selected' rooms. Above right: The former location of the L'Ecu de France restaurant on Jermyn Street, London. Interestingly, in this case both MI5 and the KGB concealed listening devices under various tables. The venue was popular with intelligence officials, diplomats and leading media people



much tradecraft was taking place at selected 'venues' in London. MI5 handymen went to work on hotel rooms, installing covert cameras, microphones and two-way mirrors. And whilst planners sought to discover if he could be simply recruited by ideology, the lure of money or eventually a better life in the West, it was evident by his actions he was only interested in female engagement. This then became a simple entrapment operation.

Embarrassing film footage, photographs and audio was secured of Grigovin. Case file officers prepared to challenge the KGB man with a carefully scripted proposal. And all the while, MI5 opted not to reveal its covert operation to its political paymasters in the event they would object and derail months of careful planning and preparation. Grigovin was a key intelligence officer who could continue in his role - passing high-end secrets to London - or defect, revealing the names of Soviet agents, traitors, moles and Kremlin intentions. His other option was less palatable and far more dangerous - he could simply explain his misdemeanours to his line officer



and return to Moscow to face the music. MI5 was confident of success.

Despite its optimism, the Security Service engaged in other planning, including exfiltration. Grigovin's family were still living in Russia, thus plans were made in the event it would be necessary to exchange agents.

When two or three burly MI5 officers caught him in another embarrassing situation, minus his clothing, he was presented with the evidence. But Grigovin stood firm. "I am a diplomat," he shouted. MI5 officers warned him that once Moscow was made aware of his behaviour, and MI5's lengthy surveillance, he would be a lost soul, and at best, just lose

his privileges. Yet he was adamant that he was not going to cooperate. Eventually driven back to his embassy, this was the last time he would be seen in the company of MI5 personnel in London.

The following morning an anonymous package arrived at the Russian Embassy. Inside were photographs of Grigovin in several compromising situations. Hours later a surveillance officer watched him being escorted onto an aeroplane by a KGB team. The Soviet spy was never heard of again. The entrapment operation had failed.

This was not the first time MI5 had engaged in such an operation, and it would not be the last. During the height of the Cold War, the Security Service used selected hotels, restaurants, clubs, bar and private meeting rooms to secure information which could be used as gateways in the ruse of entrapment. Not too dissimilar in the way in which some alleged encounters found in the Trump Dossier reveal. Do such actions and endeavours continue today? The short answer is yes. ➤



UK Defence Minister Michael Fallon

Countless services engage in elements of entrapment - the focus all in the line of duty, of course.

WEAPONISING INFORMATION

Pressure is a key element and objective of entrapment. And more recently, UK Defence Minister Michael Fallon warned that Russia is intent on "weaponising information." And though he referenced the term in respect of NATO, cyber warfare, hacking and in part, propaganda, it's a clever phrase which can be attached to some aspects of entrapment.



Another classic tale of entrapment, which was rather more successful than that deployed by MI5 against Grigovin, involved British naval attaché John Vassall (left). Based in Moscow in 1954, he was lured to a party by a sexual invitation and duly

compromised. He buckled at the thought of exposure and duly agreed to spy for the KGB. And there was even more joy for his spy handlers when Vassall was posted back to London to take a job inside the Admiralty's headquarters.

Unauthorised liaison is an area of 'no compromise', especially when government figures are posted abroad, be they diplomatic staffers, business officials, and/or intelligence officers. Protocol is a word which is often used. There are exceptions, of course, especially in the area of espionage or intelligence contact, when a deliberate deception is actioned to draw the attention of a 'person of interest'.

The word 'honeytrap' is often associated with entrapment. And spy history is laden with case files whereby a central figure is targeted using carefully managed operatives and situations. MI5 spent the best part of two



Former Europa Hotel, London where a Mossad officer was lured to his death in 1974. The incident was referenced in Steven Spielberg's iconic picture - 'Munich'



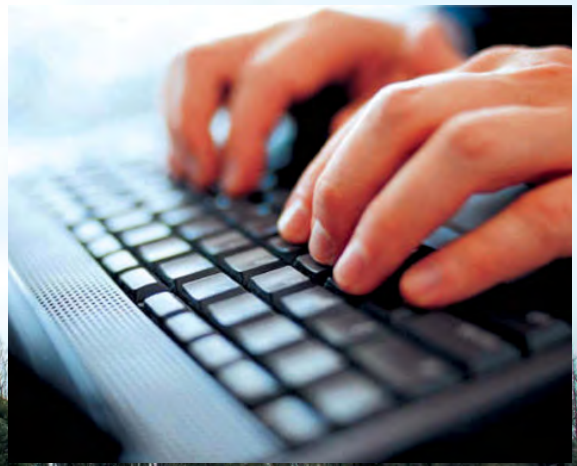
years securing all the evidence it needed to 'get' Grigovin, but quite often encounters are hurried and spontaneous affairs. These are easily identified by experienced intelligence officers, but not so by others, especially naive business persons not trained in the art of detection. A classic example of such naivety was the death of a Mossad officer in 1974. He was part of a team hunting terrorists involved in the 1972 Munich Olympic Games massacre of Israeli athletes. Staying at the Europa Hotel in London, the spy was lured to his death by a glamorous female assassin who had been hired by a proxy. Though she too was hunted down and killed by the Mossad in Holland, her actions could easily have compromised the operation. (See Eye Spy 68).

In today's technological world, there are far more opportunities for entrapment. For an intelligence employee, even receiving an unregistered cell phone call can create suspicion. And every day the real fear of cyber compromise; be it a targeted cell phone or the hacking of a personal computer, sends an additional shiver down the spine of those charged with security.

VERBAL ENTRAPMENT

Similarly, for government figures, business people and leading personalities alike, especially those engaged with the media - there is always the possibility that an 'off the cuff' remark might be picked up by a reporter, or that a microphone remains open when an interview ends. Numerous high profile figures have been caught out, but it is particularly difficult to explain or defend if such commentary occurs during a government-to-government meeting. And it is also in this 'theatre', that much underworld activity by spy agencies takes place. Be it Peter Wright's 1960s spycatchers bugging hotel phones and rooms, to today's NSA endeavours sourcing information and comments from places which Wright would believe impossible.

On the record interviews are also incredibly sensitive areas, for once the word is spoken, in many cases it cannot be retracted, thus entire organisations and personal trainers often interact with those charged with issuing comment - to make doubly sure awkward situations can be overcome. Yet it is a fact of



British diplomats and staffers attending the G20 summit in China, 2016, were warned by British Intelligence on the ruses played by China's spies. Delegates were warned of honeytraps and told to limit e-mail and computer use in the event that information could be lost leading to compromise and blackmail

life, that some in the media are intent on verbal entrapment, and are masterly in the way questions are delivered and responses manipulated.

COUNTER-MEASURES

A good example of an entrapment briefing utilising the fear factor, happened at last year's G20 Summit in Hangzhou, China. Prior to the despatch of Britain's delegation, the intelligence services spent a great deal of time briefing staff and warning delegates of Chinese intelligence operations and entrap-

ment. In this case, a previous and recent example of entrapment was used to 'spark' attention. In 2008, British Prime Minister Gordon Brown visited Beijing with his team. And during the visit, one member was allegedly drugged by a beautiful female Chinese agent, who duly removed him of his Blackberry cell phone and documents whilst the couple were 'engaged' in a hotel.*

The 2016 UK G20 delegation were warned that in all likelihood, their rooms would be bugged and cameras installed. There is also a report that suggests the staffers were advised

to don clothes under bedsheets lest they be photographed naked. Similarly, Eye Spy was informed that all electronic media (cell phones, recorders and computers) was supplied by intelligence and security specialists. The delegates were advised not to accept gifts, especially memory devices or chargers. ➤



President Bush, Director of CIA George Tenet and Secretary of State Condoleezza Rice discuss attacking al-Qaida in Afghanistan less than three weeks after 9/11

INTEL INSIDE

Throughout his presidency George Bush was a target for both his opponents and many in the press. Other dark media attempts to delve into his past also took place, including questioning his military records. However, all failed because the rumours and allegations were false. However, more difficult for Bush was his failure to find Saddam's WMD and an attempt to link Iraq with al-Qaida - thus justifying the US-led invasion.

"George Bush as a civilian, airman and president played it by the book, and made certain nothing in his past would or could be used against him," a CIA source told Eye Spy.





Premier Gordon Brown with Dmitry Medvedev in 2008

Indeed, the use of hotel computers, WiFi and external communication devices such as public telephones was prohibited. All the devices supplied by Whitehall were fitted with comprehensive cyber defences and encrypted software and passwords. And finally, no e-mails were allowed to be received from friends and family, and in cases whereby

communication was necessary with delegates, the content was to be limited.

DOCUMENTS, PAPER TRAILS

Within working environments inside intelligence buildings, the handling, distribution and managing of paper documents is strictly controlled, monitored and governed by those designated to watch over material. Incoming new files, additions and just as important, documents destined for destruction are carefully handled using security protocols which lessen the chance of espionage, compromise and entrapment. All personnel are trained to follow a methodology that has been improved over decades. However,



All platforms of information handling is an important task - any loss of data can impact significantly - be it in paper form, digital or audio

CHINESE ENTRAPMENT INTEL FRONTS AND HONEYTRAPS



In 2009, MI5's Centre for the Protection of National Infrastructure, produced a document warning of Chinese intelligence honeytraps and entrapment operations. It was directed at travelling business and government officials and others occupying senior positions within major businesses, financial houses, technology companies etc., the restricted report, titled 'The Threat from Chinese Espionage', found its way into the media.*

The report explained how the MSS was using all manner of ruses, including offering gifts such as fancy memory sticks, at business functions, trade fairs

and conferences. Of course, once attached to electronic media, the devices uploaded viruses enabling hacking. Hotel rooms were likely to be bugged and searched when unoccupied by agents who would sift through personal belongings and business items.

However, part of the report's focus was on entrapment by female operators intent on creating long-term relationships. Once this was achieved, the agents were in prime positions to exploit the situation. And of course blackmail, was referenced.

A similar warning was issued by the United States involving a Hong Kong firm - 88 Queensway Group. This was referenced by a US Congressional Committee, which said the company was a 'front that acts on behalf of the Chinese intelligence service'.

*Some intelligence watchers believe the report was 'sanctioned' for general release as a warning.

because so much material is now held on computers and passed through the Internet and internal systems, this has only led to more problems for information management controllers. A point we will explore shortly.

However, though the internal movement of information can be guarded in a closed environment such as Langley or Vauxhall Cross, this is not the case once an intelligence worker exits the door for home. And it is here that entrapment through information loss is



Corporate gifts are a popular 'token of goodwill' at Chinese business events





Security should be practised at home as well as work. Items such as SIM cards can provide a wealth of leads and contacts to unscrupulous characters. In the world of intelligence - their value is much greater

INTEL INSIDE

At the height of the Cold War, some 'out of office' social relaxation activities of MI5's Deputy Director Graham Russell Mitchell, attracted the attention of the Service's spycatchers.



A GAME OF CHESS

Mitchell was a lover of chess and would often play games with associates and friends around the world. Strange, but true, in many cases the moves of each player would be included in letters, post cards etc. At first glance this seems an innocent act, but MI5, and indeed Mitchell, was fully aware that the KGB also used such methods to communicate with its own agents around the world.

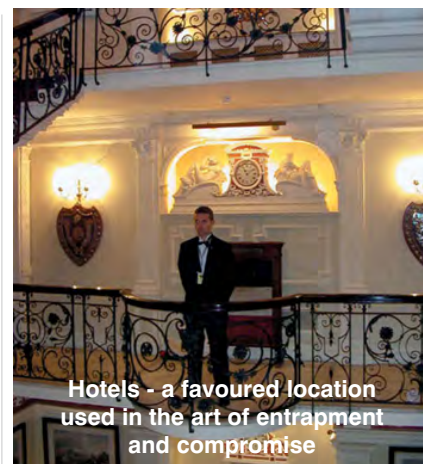
It was an avoidable indiscretion, at best a daft one. And it came back to haunt him - especially when the Service began a major bugging operation in his office, home and other locations - because they suspected he was KGB. It didn't help either that the head of MI5 at the time was Roger Hollis, also another suspected Soviet agent.

most feared. In the early 2000s, dozens of Ministry of Defence and British Intelligence laptop computers were lost by staffers. Some undoubtedly stolen. It's hard to argue against the fact that these indiscretions, accidents and thefts, left some operators open to entrapment and blackmail.

In today's 'celebrity mad world', there are lots of cases entrapment. From the taking of drugs

and excessive alcohol use, to photographing secret affairs, some in the media deliberately create environments that unwitting civilians walk straight in to. And there are countless stories involving 'dumpster diving' by unscrupulous reporters and even fans. From examining food packaging to identifying favourite reading material, acts take place which are annoying, innocent, inquisitive and distasteful. But when the objective has a more covert purpose, then the incident takes on new dimensions, and this is most relevant when entrapment in the intelligence world takes place.

In intelligence work, staffers and officers are warned endlessly about personal protection, from destroying receipts, telephone numbers, erasing electronic media, burning bank statements, use of ATMs and even holiday brochures - all to ensure anonymity. Nevertheless, when an entrapment operation is engaged, all manner of acts take place to secure information, from surveillance of favourite locations, activities, meeting friends and associates, banks, car hire etc. The list is



Hotels - a favoured location used in the art of entrapment and compromise

truly lengthy. The primary intention is to build up a character profile and lifestyle. With such information at hand, planners can focus on identifying areas for future exploitation.

And unbeknown to many, these are ordinary actions and liaisons which can in future days lead to compromise.

Continued on page 78



INTEL INSIDE

Left: President Trump, with Vice President Mike Pence (left) and Secretary of Homeland Security John Kelly. All the men are fully aware that covert and overt attempts continue to link members of his inner circle and senior officials to Russian Intelligence - thus raising suspicion of interference, collaboration and underhand tactics in the 2016 General Election. Mr Trump is convinced that some media houses are being provided with leads from inside the United States Intelligence Community (USIC), though it's very unlikely these channels will ever be identified publicly

BEHIND CLOSED DOORS

INTEL DETENTE?

Confusing statements as Russia and NATO seek a platform for intelligence sharing, dialogue and a lessening of tensions



Speaking to a gathering of FSB officials and officers in Moscow, Russian President Vladimir Putin said it is about time the intelligence services of Russia and the West

improve relations to combat the menace of international terrorism. His outreach lecture was delivered just eight weeks after the United States expelled 35 Russian diplomats and spies from its Washington Embassy, including a number of senior FSB and GRU intelligence officers. It also coincided with much turmoil in America following the resignation of President Trump's National Security Advisor Michael Flynn, who many believe was "too friendly towards Russia."



Mr Putin said it would be in the best interests of NATO countries and Russia to "open up lines of communication." He warned NATO forces were forever provoking his country and attempting to draw Moscow into conflict. Putin saw a similarity to the climate of the Cold War: "NATO has a new mission - to deter Russia. This is the goal behind the expansion of the military bloc. It happened before, now they have found a new justification which they believe to be serious." He went on to say that the Alliance is engaged in a major programme to "interfere with domestic affairs... the objective being to destabilise Russia."

Relations between the West and Russia have been deeply affected by events in the Ukraine, increasing tension in Baltic states and a failure to agree on how best to tackle ISIS in Syria and elsewhere. "It's in everyone's interest to resume dialogue between the intelligence agencies of the United States and other members of NATO," said Putin. "It's absolutely

US and Polish security services engage in a joint exercise in Poland. Both the USA and UK have several thousands troops now in the country - a warning no doubt to Russia



clear that in the area of counter-terrorism, all relevant governments and international groups should work together."





Defence Minister Sergei Shoigu



Russian-backed militia in Ukraine continue to pose a problem

President Trump has already said he wants better relations with Russia, and that it would be in the "best interests of the international community if a cohesive plan was created to tackle ISIS." And Putin sees such language as an opportunity to re-build bridges. "Further steps towards the restoration of Russian-American relations will be built on the basis of the policy which the administration of President Trump will carry out," he said.



Russian-backed militia celebrate the downing of Malaysian Airlines Flight MH-17 in 2014 in eastern Ukraine. Investigators proved it was brought down by a Russian-built mobile Buk surface-to-air system

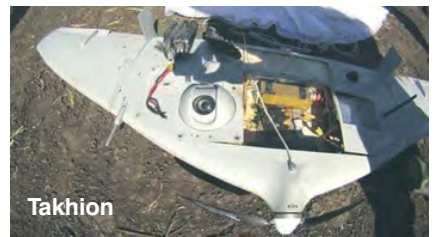
DECEIVED BY FLIGHT

KIEV: The images produced by the security services in Ukraine, show various Russian UAVs recovered in the east of the country where tensions remain high. Ukraine Intelligence state the UAVs were used in a surveillance role to help Russian artillery units target specific sites - unfortunately some occupied by civilians.

Ukraine has identified several senior Russian commanders allegedly involved in war crimes, and has accused personnel of Russia's GRU intelligence service (Reconnaissance Group) of "murderous acts."



Forpost



Takhion



Eleron-3SV



Orkan-10



US Secretary of Defense James Mattis with King Abdullah II of Jordan. Inset: Mattis arrives at the Pentagon on his first day in office



Baltic troops mix with civilians whilst performing a defensive exercise

Of additional interest to espionage watchers, during his talk to the FSB, Mr Putin also said that his intelligence services had “thwarted over 400 foreign special agents.” Though he failed to elaborate on their supposed activities, he did say 53 were foreign intelligence operatives and 386 were agents belonging to foreign intelligence services. Eye Spy associates in Moscow said several worked at foreign embassies.

‘TIT-FOR-TAT’ CHAT

Russia’s Defence Minister Sergei Shoigu has also engaged in the debate on future Russia-United States cooperation. Following comments by new US Defense Secretary James Mattis, who said he wanted American diplomats to “hold the upper hand” in any talks with Russia, Shoigu said: “We are prepared to restore cooperation with the Pentagon, but attempts to establish dialogue

from a position of strength would be fruitless.” However, Mattis, a former Marine Corps General then responded with a comment that at first examination seemed to reveal fractures will exist for some time. “We are not in a position right now to collaborate on a military level. But our political leaders will engage and try and find common ground.”

All of this comes at a time when NATO continues to bolster security on its eastern and northern flanks, and much discussion ensues about member nation funding.

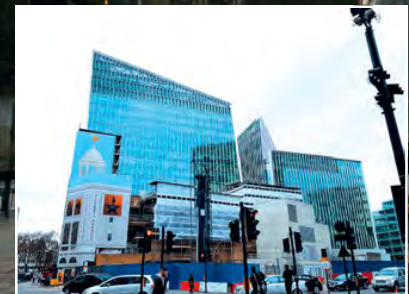
- In March 2017, NATO and Russian officials met to discuss various intelligence-related issues for the first time since relations were frozen in 2014. Topics included the prevention of incidents and details of several major Russian military exercises to be held later this year close to NATO positions.



Russian Defence Minister Sergei Shoigu and Syrian officials discuss operations at Khmeimim air base near Latakia, Syria

NATIONAL CYBER S

ING



IN DEFENCE

National Cyber Security

SECURITY CENTRE

NCSC



“The NCSC will play a unique and crucial role bringing together the public and the business community on the one hand, and our intelligence and security agencies on the other...”

CE OF THE

urity Centre Officially



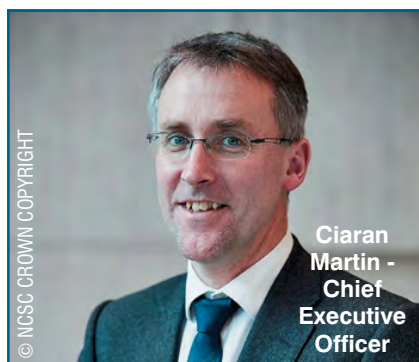
HM The Queen with Robert Hannigan, Director GCHQ, and Ciaran Martin, CEO National Cyber Security Centre

The centre, which is a part of GCHQ, headed by new cyber security chief Ciaran Martin, was officially opened in February, by Her Majesty The Queen accompanied by His Royal Highness The Duke of Edinburgh.

The centre's aim, is to “make the UK the safest place to live and do business online,” said Mr Martin. “We will help secure our critical services, lead the response to the most serious incidents and improve the underlying security of the Internet through technological improvement and advice to citizens and organisations.”

MERGING HOUSES

NCSC brings together and replaces three existing cyber security organisations: Centre



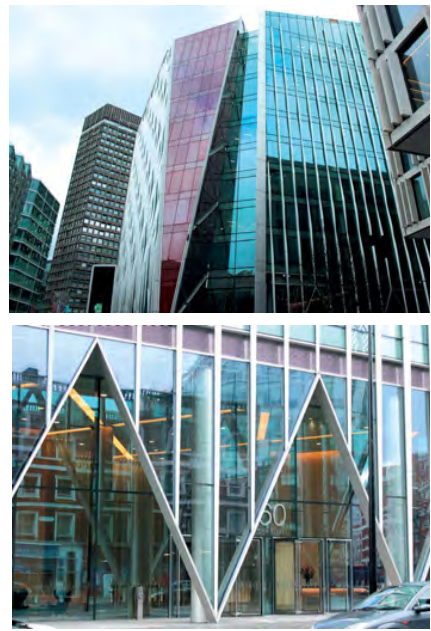
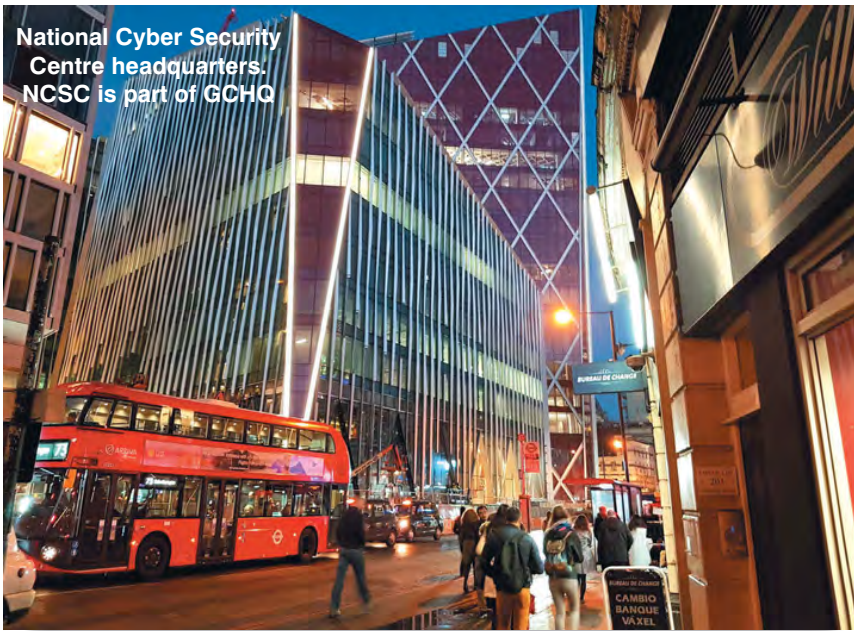
for Cyber Assessment (CCA); Computer Emergency Response Team UK (CERT UK) and CESG (GCHQ's information security arm). It also includes the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI).

Technical director, Dr Ian Levy, said: “We recognise that, despite all our efforts to reduce risks and enhance security, incidents will happen. When they do, the NCSC will provide effective incident response to minimise harm to the UK, help with recovery and learn lessons for the future. NCSC will work together with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management. This is underpinned by world-class research and innovation.” ➤

INTERNET REALM

Opened by Her Majesty The Queen

National Cyber Security Centre headquarters. NCSC is part of GCHQ



HM The Queen views items from GCHQ's archives

HM The Queen officially opens NCSC. Inset: Robert Hannigan, Director GCHQ and Ciaran Martin, CEO National Cyber Security Centre



Embedding good practise in all computer users is a primary objective of NCSC, and its strategy is to "use government as a guinea pig for all the measures we want to see done at a national scale," said Levy.

NCSC was established to bridge industry and government, with the aim of providing a single source of advice and support on cyber security, including the management of cyber security incidents.



Phillip Hammond

Also at the opening, Chancellor Phillip Hammond, who discussed plans for a new partnership for private sector organisations and the NCSC. "We will invite businesses up to 100 employees to come and work in the NCSC - allowing us to draw on the best and the brightest in industry - to test and challenge the government's thinking as we take this project forward," Hammond said. "The NCSC will play a unique and crucial role bringing together the public and the business community on the one hand, and our intelligence and security agencies on the other. Second, it will focus on partnership."

The NCSC has been operational since October last year and has already responded to 188 cyber attacks. The new headquarters is based in Victoria, London, and when fully operational, will be staffed by around 700 employees. No doubt including some of those participants in the Cyber Security Challenge reported upon by Eye Spy (see issue 105).

GCHQ PREPARE CENTENARY CELEBRATIONS

In two years time Government Communication Headquarters (GCHQ) will celebrate its 100th anniversary. Founded as the Government Code & Cypher School in 1919, its title changed in 1946.



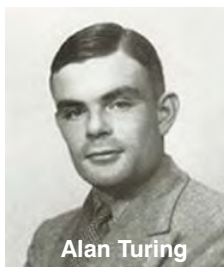
GCHQ intends to mark the day by holding various events and activities covering science, secrets, and of course - subterfuge. The organisation has also commissioned Professor John Ferris to write its first authorised history. Ferris, a well known intelligence and security expert, will examine its origins and history, and cover important dates beginning in World War One; WWII activities at

**GCHQ headquarters. Below right:
Recovered German WWI codebook**



Work begins on GCHQ headquarters building, Cheltenham 1950s

Foyer of GCHQ building 2017



Alan Turing

Bletchley Park codebreaking centre; the Cold War through to the present day.

There will also be a privately funded exhibition at the Science Museum in

London, where visitors will be able to play with some of the gadgets; see never before released secret papers from the archive and study the work of leading cryptographic figures such as Denniston, Tiltman, Turing, Clarke, and Ellis.

In 2016, GCHQ gave £30,000 to charity from money raised from sales of a special book focusing on the life and work of perhaps the world's greatest codebreaker - Alan Turing. L-R. Pictured is the book's author, Sir Dermot Turing (nephew of Alan), former C of MI6 Sir John Scarlett, GCHQ historian Tony Comer, who has been commissioned to write the organisation's official centenary book, and Christopher Moore, Deputy Chairman of the Bletchley Park Trust

Though today headquartered in Cheltenham, the organisation has links to numerous intelligence, defence and research sites across the country, including signals facilities. These too will be recognised and explored.

GCHQ Historian Tony Comer said: "GCHQ has kept Britain safe for 100 years, and will keep doing so into the future. Our centenary is a

unique moment to commemorate our past, tell you more about what we do, and celebrate the people who have made GCHQ such a ground-breaking place to work for 100 years.

"It wouldn't be GCHQ without a puzzle, so although we promise to keep you up to date on our centenary plans, you might need your codebreaking skills for the next instalment."



CHANGING TIMES



Intelligence and security appointments reflect changing dynamics of a domain once totally dominated by males

Whilst the role of females in the world of intelligence and espionage has always been recognised, few women before the 1990s, were ever considered for the top job in an intelligence agency. This male 'corridor' mentality changed in the 2000s, when MI5 appointed its first female head in the person of Stella Rimington. A few years later the Service soon had another woman lead the Service - Elizabeth Manningham-Buller.

Elizabeth Manningham-Buller



37% of all British Intelligence (MI6, MI5 and GCHQ combined) workers are female - this is set to increase to nearly 50% by 2022

Today, agencies such as the CIA, MI6 and the Mossad, to name but three, are engaged in projects to secure the services of more female intelligence workers. Therefore it is inevitable, and with good and authentic cause, perhaps in the next decade, a female will be appointed head of these very secret foreign intelligence collection services.

The increasing visibility of females in the security and intelligence spotlight, has been evidenced in recent weeks: Cressida Dick,

New Scotland Yard (NSY), Gina Haspel, CIA and Stephanie O'Sullivan, Office of the Director of National Intelligence (ODNI) have all been in the news.

RETURN OF CRESSIDA DICK

Cressida Dick, 57, who joined NSY in 1983, departed in 2015 to take a position at the Foreign Office. She was one of four candidates to be considered for the position of NSY commissioner, following the departure of Sir



Stella Rimington - first ever female Director-General of MI5

Bernard Hogan-Howe. Now she heads a force of 43,000 officers and staffers. She came to the public's attention as gold commander of the operation which resulted in the shooting dead of Brazilian electrician Jean Charles de Menezes. In this case de Menezes was



Cressida Dick

mistaken for a terrorist suspect shortly after several al-Qaida bombers attacked sites in London in July 2005. Sir Bernard Hogan-Howe described Dick as a "role model for women in the



Charles de Menezes



Cressida Dick is flanked by London Mayor Sadiq Khan and Home Secretary Amber Rudd

Service." Interestingly, her position at the Foreign Office was never fully understood by intelligence watchers.

GINA HASPEL

In Washington, CIA Director Mike Pompeo announced he has appointed Gina Haspel as Deputy Director. Although not the first female to hold this position, Haspel is the first female career CIA officer who has risen through the



CIA employment banner

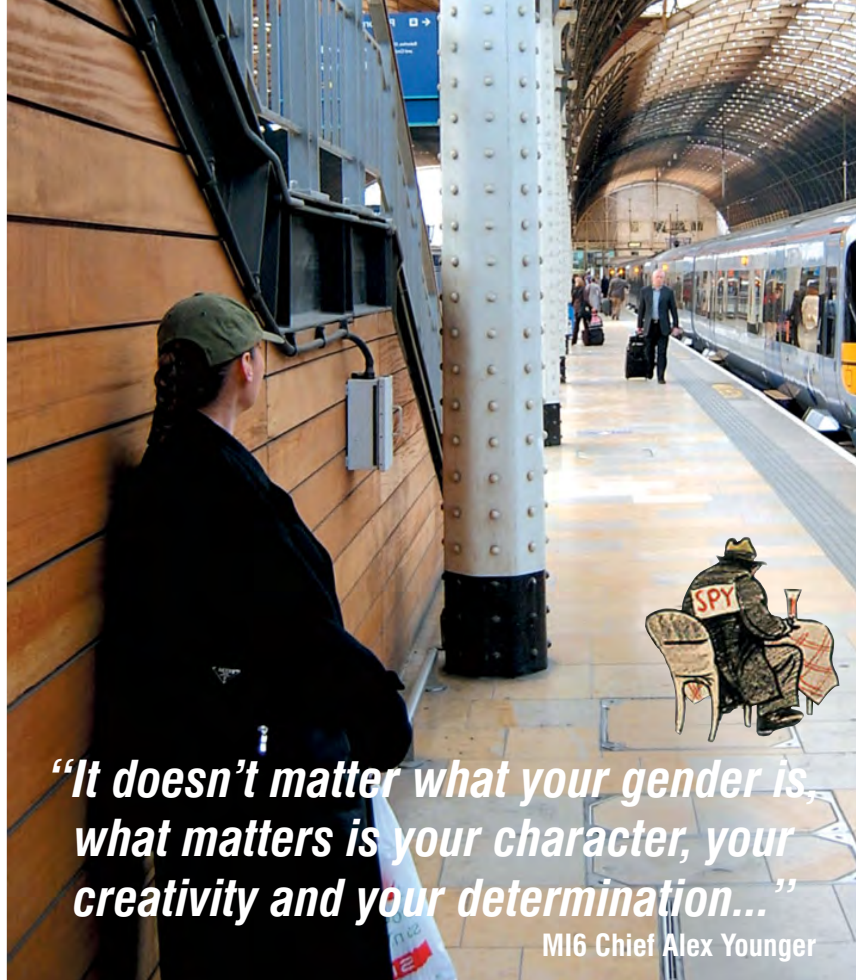
ranks to take the position. She joined the CIA in 1985. Haspel has extensive overseas experience, held several top senior leadership positions and served as Deputy Director of the National Clandestine Service for Foreign

Intelligence and Covert Action - Langley's creative spy arm.

Haspel's appointment has drawn criticism from some in Washington due to her role in the CIA's extraordinary rendition programme. However, she is the recipient of numerous awards including the George H. W. Bush Award for excellence in counterterrorism; the Donovan Award; the Intelligence Medal of Merit; and the Presidential Rank Award.

"Gina is an exemplary intelligence officer and a devoted patriot who brings more than 30 years of Agency experience to the job," said Director Pompeo. "She is also a proven leader with an uncanny ability to get things done and to inspire those around her. We are fortunate that someone of her intellect, skill, and experience will be our Deputy Director. I know she will do an outstanding job, and I look forward to working with her closely in the years ahead."





STEPHANIE O'SULLIVAN

Another senior female US intelligence officer has also made headlines. Principal Deputy Director of National Intelligence, Stephanie O'Sullivan, has announced she is to leave her post at the Office of the Director of National Intelligence (ODNI). Always one to keep a low profile, O'Sullivan, like Haspel and Dick, she too rose through the ranks and has spent most of her life working on behalf of the United States Intelligence Community (USIC). Her decision to depart is not political, and closely follows the resignation of her superior - ODNI head James Clapper.

The NRO (National Reconnaissance Organisation) and NGA (National Geospatial Intelligence Agency), are two ultra secret US organisations. In 2010, Letitia Long was appointed head of the NRO, and today, Susan Gordon serves as Deputy Director of the NGA.

The Defense Intelligence Agency (DIA), has also recently announced that its new Deputy Director is a female, in this case long-time career intelligence officer Melissa Drisko. She served as Deputy Director of the Office of Naval Intelligence (ONI) and has worked for the CIA and the State Department's Intelligence Bureau.

REFLECTIONS

On MI6's website, the Service has a very brief section on its history. However, within the period 1914-1918, there is reference to its first Chief - Sir Mansfield Cumming and how MI6 was reliant upon women working as secretaries, typists, clerks and drivers. Typical of the period, but today, the role of women in intelligence is a world away from that encountered by their predecessors. This is reflected by comments made in January 2017, by MI6 Chief Alex Younger, speaking at the Women in IT Awards in London. He revealed the head of the Service's technical services section (equipment), is a female. In an effort to encourage more females to join the intelligence world, Younger told the audience: "The real-life 'Q' is looking forward to meeting you... and I'm pleased to report that she is a woman."

Mr Younger summed up the position which probably reflected the viewpoint of most people who oversee or work in Intelligence: "It doesn't matter what your gender is, what matters is your character, your creativity and your determination."



• *Though a recent report by the UK Intelligence and Security Committee revealed 37% of people working for all arms of British Intelligence are female, there was no breakdown in respect of positions held.*



"In my experience, changing organisational culture is the most challenging aspect of leadership..."

ODNI Stephanie O'Sullivan





MI6 Chief
Alex Younger

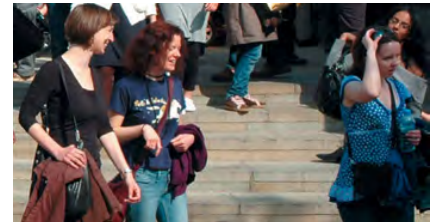
Framed image of women
purportedly working for
MI6 around 1919

DO NOT RESTRICT INTEL SEARCH CRITERIA



Government Response to the Intelligence and Security Committee of Parliament Report on Women in the UK Intelligence Community

In 2016, the British Government published a report regarding women in the intelligence arena. Titled: **'Government Response to the Intelligence and Security Committee of Parliament Report on Women in the UK Intelligence Community'**, the authors made several significant recommendations.



In the arena of recruitment, the report said: *'Targeting specific groups of women to recruit. The Agencies should explore groups other than graduates. Women or mothers in middle-age or mid-career, who may have taken some years out to bring up children, may offer an untapped recruitment pool. The Agencies should use a broad range of mediums to advertise, including those specifically for women and mothers such as Mumsnet. The Agencies should examine their entry criteria. Many middle-aged women will have life experience but not necessarily the standard qualifications: which is more important?'*

that the 'tap on the shoulder' method is important - especially to secure the services of people with the 'right stuff'."



MI6 said the girl featured in
the film is not an employee



NEW THREATS AND THE PRIVATE SECTOR

For several years MI6 has endeavoured to distance itself from the pre-conceived 'tap on the shoulder' in respect of recruitment. This once overly secretive organisation has launched several new initiatives in an effort to attract different types of candidates. One such project is a film advertisement which is being shown in cinemas in London and parts of Britain. It features a young woman of ethnically indeterminate background demonstrating people skills and emotional intelligence in a range of everyday situations. The female, *'does not work for MI6... but she could'*, the advert states.

MI6 sources explained the Service is keen to remove itself further from the archetypal 'Bond' image, calling it a "grotesquely misleading stereotype." MI6 Chief Alex Younger said: "Simply, we have to attract the best of modern Britain. Every community from every part of Britain should feel they have what it takes, no matter what their background or status. We have to stop people selecting themselves out."

He also commented about new tasks and dangers facing the intelligence world, and how adversaries are exploiting technologies. "The



A still from the MI6 recruiting film

information revolution fundamentally changes our operating environment. In five years time there will be two sorts of intelligence services: those that understand this fact and have prospered, and those that don't and haven't. And I'm determined that MI6 will be in the former category."

MI6, MI5 and GCHQ senior officials have expressed concerns about losing officers and ideal candidates to the private sector, including business intelligence companies where financial rewards are generally much higher. One official described the situation as "alarming." Interestingly, this drift of employees and preferred candidates is mirrored by the intelligence community in North America.

An intelligence watcher with an insight into MI6 recruitment told Eye Spy. "Despite website engagement with the public, MI6 still recognise

DEEP BLACK

Extraordinary Rendition

Alleged MI6 threads to abduction set to be heard in court as ripples from secret CIA programme continue to expand

In a landmark legal decision which is of concern to MI6 and some of its officers, Britain's High Court has said it will hear an application for a judicial review of the Crown Prosecution Service's (CPS) decision not to bring charges against the Service's former Counter Terrorism Director Sir Mark Allen over the abduction of anti-Colonel Muammar Gaddafi opponent - Libyan Abdel Hakim Belhaj. Belhaj had fought with the Libyan Islamic Fighting Group (LIFG) which sought to topple the dictator in the 1990s. He later fled to Afghanistan. The United Nations designated the LIFG a terrorist group after links with al-Qaida were identified.

Belhaj and his pregnant wife, Fatima Boudchar sought asylum in the UK whilst living in China in 2004. They were detained in the Far East just before embarking on a flight to Britain. The couple were handed over to the CIA whilst



Sir Mark Allen

in Bangkok, along with another Libyan, Sami al-Saadi, who was detained in Hong Kong (see Eye Spy 78). It is alleged Langley was tipped-off about Belhaj's whereabouts by



Abdel Hakim Belhaj

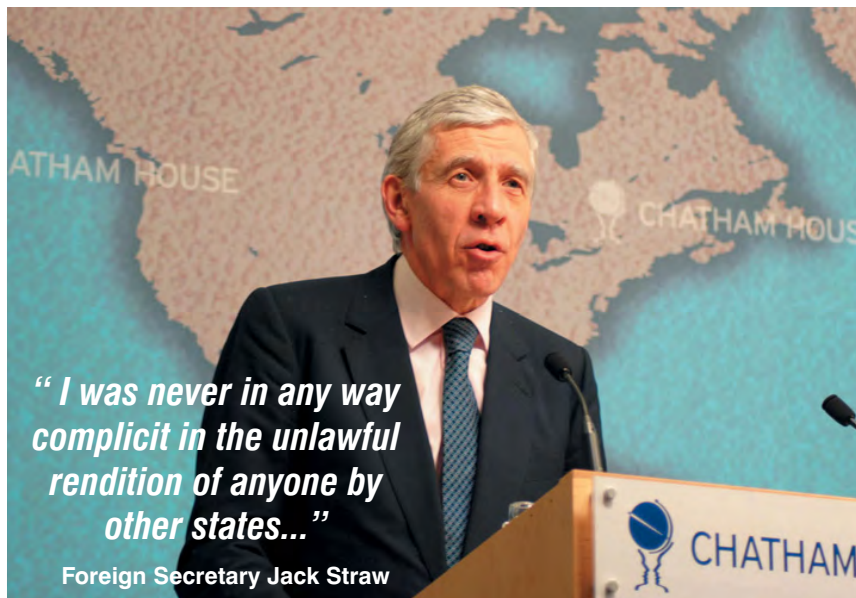
MI6 agents. Thereafter allegations of torture and mistreatment at a Langley Black Site were made. At the time, both men were regarded by the CIA as terrorist suspects.

After a short time in Bangkok, the Belhajs were flown to Libya and held at the notorious Abu Salim prison. More interrogations ensued by agents, some of whom were alleged to be British. Boudchar was released following the birth of their child, but he was held for a further four years before being sentenced to death. However, despite political turmoil on the horizon, Belhaj was released in 2010 along with other LIFG members. Gaddafi's son, Saif al-Islam, said he was "no longer a threat to the country."

THE FALL OF GADDAFI

In 2011 the Arab Spring erupted and within months Gaddafi's regime was toppled. In August of the same year, Belhaj was appointed commander of the Military Security Council responsible for public and government security in Tripoli. Documents were then discovered by anti-Gaddafi fighters in a building used by Libya's former intelligence service, some were passed to the media, including journalists at the *Guardian* and BBC. At least one referenced MI6, Libya's former spy chief Musa Kusa - and former Prime

GUANTANAMO BAY



"It is in the Service's interest to deal with the allegations being made as swiftly as possible so we can draw a line under them and focus on the crucial work we now face in the future."



Minister Tony Blair's visit to the country in March 2004. A letter, dated 18 March 2004, and allegedly written by MI6 CT chief Sir Mark Allen read: 'Most importantly, I congratulate you on the safe arrival of Abu Abd Allah Sadiq (Abdel Hakim Belhaj). This was the least we could do for you and for Libya to demonstrate the remarkable relationship we have built over the years. I am so glad. I was grateful to you for helping the officer we sent out last week'. The British Government has never confirmed its authenticity or if it regards it as bogus.

Following Gaddafi's demise, stories about alleged MI6 involvement in the rendition of Belhaj started to surface. Then Foreign Secretary Jack Straw denied any knowledge of the rendition. He too is caught up in the legal happenings. Speaking through his solicitor, Mr Straw said: "As Foreign Secretary I acted at all times in a manner which was fully consistent with my legal duties, and with national and international law. I was never in any way complicit in the unlawful rendition of anyone by other states."



Belhaj later said he was "surprised" that some of the first people to interview him were British intelligence officers. Indeed, he supposedly recognised one officer. And then in December 2011, legal proceedings were initiated by Belhaj against some British Government figures. In 2013, a judge ruled that whilst Belhaj had a "well founded case," pursuing it would "jeopardise national security," hence the decision not to proceed. A solicitor representing Belhaj said: "If this judgement





Colonel Muammar Gaddafi

stands, it will mean that anything our security services do alongside the US Government is totally immune from the British legal system, even if MI6 officers arrange the rendition of a pregnant women into the arms of Gaddafi." Belhaj wanted just £1 in compensation and an apology.

DEAL IN THE DESERT

Reprieve, the organisation representing Belhaj, believes the alleged collaboration was part of a wider collective known as the 'deal in the desert', which followed the meeting of Tony Blair and Colonel Gaddafi. All manner of legal hearings, accusations and damage limitation have since followed. And to complicate matters further, New Scotland Yard's comprehensive investigation into the affair, codenamed Operation Lydd, initiated on 5 January 2012, is said to have contained information that some believed should have been actioned in a court room. When news first surfaced about the investigation, then MI6

Chief Sir John Sawers said: "It is in the Service's interest to deal with the allegations being made as swiftly as possible so we can draw a line under them and focus on the crucial work we now face in the future."

Belhaj's team allege that whilst he was held in detention, "the UK and security and intelligence services sought and obtained access to them and interrogated them, in circumstances where it was obvious that they were being held incommunicado, without any judicial supervision, and were subject to mistreatment and torture." However, in June 2016, and in receipt of the New Scotland Yard investigation, Sue Hemming, head of the CPS's Special Crime and Counter Terrorism Division said: "Following a thorough investigation, the CPS has decided that there is insufficient evidence to charge the suspect with any criminal offence."



Abdel Hakim Belhaj - wanted £1 and a British Government apology



Gaddafi's spy chief Musa Kusa was an MI6 contact man

This decision has now been challenged and even if a new judicial review is rejected, documents regarding the case could still be requested and used.

The rendition of Belhaj came at the height of Langley's global hunt for terrorists following 9/11, and involved the use of buildings and compounds often situated close to airports. These allowed for secret interrogation and movement of suspects.

Sir Mark Allen, now retired, is a well-respected and experienced intelligence officer; once a favourite for the position of 'C' of MI6, he denies any wrong-doing.

And for the record, Eye Spy was informed 20,000 top secret British Intelligence documents were examined following allegations of "wrong-doings" after 9/11. A judge found no evidence UK intelligence officers were "directly involved in the torture or rendition of suspects."

20,000 top secret British Intelligence documents were examined following allegations of "wrong-doings" after 9/11. A judge found no evidence British intelligence officers were "directly involved in the torture or rendition of suspects"

THE 'IMAM RAPITO AFFAIR'



Former CIA Agent 'Pardoned' by Italian President Mattarella

Italian President Sergio Mattarella has effectively pardoned former CIA agent Sabrina De Sousa, 61, convicted of involvement in the kidnapping of Egyptian cleric Osama Moustafa Hassan Nas, known as Abu Omar. An Italian court had ruled she had taken part in the kidnapping of Omar, a suspected al-



Abu Omar

Mattarella granted a partial pardon reducing De Sousa's four year sentence

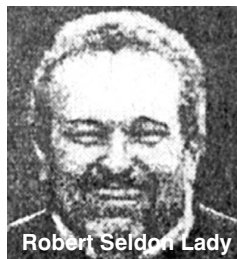
Qaida operative in Milan 14 years ago as part of the CIA's extraordinary rendition anti-terrorism programme.

In a statement released by the President's office,

(originally seven years) by a year to three-years, without the need to serve a prison term.

The statement said Mattarella had based his decision on "the attitude of the sentenced party, the fact that the United States has discontinued the practice of extraordinary renditions and the need to weigh up the penalty with that of others convicted of the same offence".

De Sousa was one of 23 CIA operatives, including Robert Seldon Lady, the Rome Station Chief convicted in the case, better known as the 'Imam Rapito Affair', but the only one to



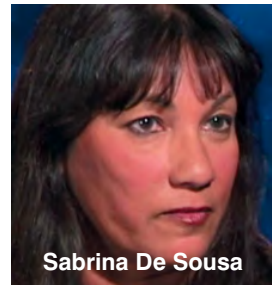
Robert Seldon Lady



CIA surveillance photo of Abu Omar

serve jail time. The other Americans have also received clemency.

De Sousa can now apply to serve her sentence under house arrest or performing social work.



Sabrina De Sousa

In Washington, former Michigan Congressman Pete Hoekstra, who has been liaising with the former spy, her husband and the Trump administration, said the hope was she would be allowed to serve three years of community service in Portugal where she was being held. De Sousa entered Portugal in 2015 as she made her way to see her sick grandmother in India. During the stopover, she was detained by police

De Sousa has always denied any involvement in the operation and for two years has fought extradition. Her legal team has argued that because of her former status, she cannot use government documents to prove her innocence.

GUANTANAMO REBOUND

The Million Pound Bomber

Freed British Guantanamo Bay Detainee Attacks Iraq Army Post



Frame from an ISIS video showing Ronald Fiddler in his vehicle readied for a suicide attack near Mosul

A British man detained by US Special Forces in Afghanistan in 2001, and held at Guantanamo Bay Prison for two years before being released, has attacked an advancing Iraq Army unit near Mosul on behalf of ISIS. Ronald Fiddler, from Manchester died in the operation after he detonated a car packed with explosives. During his time in the Cuban jail, Fiddler provided useful information on the Taliban to his CIA handlers. Indeed, the Taliban initially thought he was a British agent. As for his being in the region in the first place, he said he was on a backpacking trip.

Following his relocation to the prison in 2001, there was much debate in the UK about Fiddler, and several human rights groups and activists campaigned for his release. ➤



Indeed, at the time they were supported by various journalists and British politicians, including then Home Secretary David Blunkett. And though much suspicion ensued about his ties to terrorism, with no hard evidence he was freed. At the time, Mr Blunkett said: "No one who is returned will actually be a threat to the security of the British people."

Part of a letter written by Fiddler following his release states: *'The irony is that when I was first told in Afghanistan that I would be in the custody of the Americans, I was relieved as I thought I would be properly dealt with and returned home without much delay.'*

'I have never been in any kind of trouble with the law and have never engaged in any kind of



ISIS armoured suicide vehicle

fighting or planning or participating in any kind of violence or terrorist behaviour'.

Fast forward over a decade from the mountain pathways that straddle the border regions separating Pakistan and Afghanistan to the battlegrounds in and around the city of Mosul. Here Iraqi forces are engaged in fierce fighting with well-armed ISIS terrorists. Fiddler, A.k.a. Abu-Zakariya al-Britani and Jamal al-Harith, drove to an Iraq Army holding camp in Tal Gaysum to the southwest of the city. As he approached troops he detonated a large bomb contained within the vehicle. It was an audacious attack and one that ISIS was keen to exploit using the Internet to highlight the 'brave actions of the Briton'. Three other car suicide bombers also attacked various Iraqi positions killing several soldiers and wounding many more.

FIDDLER'S ROAD TO ISIS



Ronald Fiddler killed an unspecified number of Iraqi troopers

It transpired that Fiddler journeyed to Turkey in early 2014, before crossing into Syria. Here he joined ISIS, signing various papers which designate him as a 'volunteer fighter of Islamic State'. These papers are in the possession of MI6 and MI5, along with the names of around 1,000 Britons who have joined the terror group. A year later he was joined by his wife, Shukee Begum and their five children. She said they had tried to convince him to return to the UK. For the next few months she endeavoured to leave, but was stopped by ISIS and other groups. Eventually she was reportedly 'rescued' by the al-Qaida franchise Al Nusra terror group.

Following news of Fiddler's death in February 2017, it transpired that he received around £1 million in compensation from the British Government in 2010. This was supposedly because British Intelligence, aware of his

Images such as this have not helped the reputation of Guantanamo Bay prison facility



Evidence of the fierce fighting in Mosul, Iraq. Inset below: ISIS terrorists fire from a captured US Humvee armoured vehicle (propaganda image)



"There was absolutely no merit in paying him a penny because plainly he was a terrorist and a potentially dangerous terrorist..."

Lord Carlile





Prisoner interview watching station, Guantanamo Bay



US Marine General Joseph Dunford and troops from the Iraq Counter Terrorism Service (CTS) display an ISIS flag captured from terrorists on the outskirts of Mosul



Iraq soldiers with grateful residents in eastern Mosul

detention at Guantanamo Bay without charge, knew he was being mistreated. However, a more likely reason exists: that if a court action was enabled to secure compensation, there was a very real possibility secrets and intelligence could be compromised.

Commenting on yet another freed Guantanamo inmate engaged with terrorism

(called a Recidivist), former independent reviewer of terrorism legislation, Lord Carlile, believes the Mosul incident is evidence enough that Fiddler should not have received £1 million compensation. "There was absolutely no merit in paying him a penny because plainly he was a terrorist and a potentially dangerous terrorist."

INTEL INSIDE

Todate, around 700 inmates have been released from the US run, Cuban-based prisoner holding facility Guantanamo Bay. According to US intelligence estimates, nearly 20% have returned to terrorism, whilst a further 13% are suspected of rejoining terrorist groups - about one third if the figures are merged.



BLACK SITE MISCHIEF WHITE HOUSE DENIES 'RE-RUN' PAPER

A purported White House draft executive order appeared on WikiLeaks and was widely reported upon by some US media outlets calling it a 'leaked briefing'. The document suggested President Trump was considering a major review of methods for interrogating terror suspects and the possible reopening of CIA-run 'black sites' outside the USA.

White House Press Secretary Sean Spicer said that the draft

executive order on US interrogation methods did not originate from the White House. "It is not a White House document," Spicer said at a briefing. "I have no idea where it came from, but it is not a White House document."

In a statement, Senator John McCain, who was held captive during the Vietnam War, said that the CIA's new director Mike Pompeo, pledged in his recent confirmation hearing before the Senate that he would "comply



2006. Lt. General Keating US Army, with new Field Manual (FM) 2-22.3 - 'Human Intelligence Collector Operations'. Rules prohibit many controversial enhanced interrogation techniques, including 'waterboarding'

with the law that applies the Army Field Manual's interrogation requirements to all US

agencies, including the CIA." US Defense Secretary James Mattis vowed the same.

WATERGATE II

THE 'BUGGING' OF TRUMP TOWER



Allegations of surveillance, telephone tapping, secret contacts, mistrust and mischief abound in Washington

Dan Rather, the American journalist who for over two decades fronted CBS Evening News, believes President Trump's pre-election liaisons with Moscow, could well turn out to be a bigger political scandal than Watergate. Speaking about the election, Russian hacking and the recent resignation of Trump's National Security Advisor, Michael Flynn, Rather said: "Watergate is the biggest political scandal of my lifetime, until now... maybe." He recalled the break-in at the Democratic National Committee (DNC) headquarters at the Watergate complex in Washington DC in 1972, saying it was "the closest we came to a debilitating Constitutional crisis."

Rather believes more news stories will emerge in future days about several associated issues, including the inter-action between several President Trump figures and Russian officials. This will only serve to heighten mistrust. Comparing the two affairs, Rather added: "On a 10 scale of Armageddon for our form of government, I would put Watergate at a 9. This Russia scandal is currently somewhere around a 5 or 6, in my opinion. But it is cascading in intensity seemingly by the hour."

When five men broke into the DNC headquarters at the Watergate complex in Washington, it was quickly linked to President Nixon and his aides. Thereafter several senior Nixon

Radio transmitter and walkie-talkie - exhibits from the Watergate investigation -



Dan Rather

administration officials were indicted for criminal offences. Asked about his knowledge of the break-in, Nixon initially denied any connection or knowledge, but the incident developed into a major political scandal, eventually resulting in his resignation.

"When we look back at Watergate, we remember the end of the Nixon Presidency," said Rather. "It came with an avalanche, but for most of the time my fellow reporters and I were chasing down the story as it rumbled along with low-grade intensity. We never were quite sure how much we would find out about what really happened. In the end, the truth emerged." Rather believes a similar situation could develop involving the Trump administration. "We need an independent investigation."





President Trump speaks with US sailors as he attends a gathering at the soon-to-be commissioned aircraft carrier USS Gerald R. Ford



We may look back and see in the end, that it is at least as big as Watergate. It has all the necessary ingredients, and that is chilling.”

President Trump meanwhile, caused uproar on both sides of the Atlantic when he accused his predecessor of organising a telephone tap operation targeting systems in Trump Tower, New York, just weeks before the General Election concluded. He too referenced Watergate in a another controversial ‘tweet’: ‘How low has President Obama gone to tapp my phones during the very sacred election process. This is Nixon/Watergate. Bad (or sick) guy!’ Another related Trump ‘tweet’ described the tapping as ‘McCarthyism’. The word has various popular meanings and



FBI Director James Comey rejected the President’s claims

originates from the early Cold War days in which Senator Joseph McCarthy raised already existing tensions in the country about

suspected US nationals who supported Communism or were spies.* It can mean accusations of treason, subversion and skulduggery



Joseph McCarthy

- all made without proof. However, Trump probably focused on its meaning of ‘using unfair investigative techniques’. During the so-called Second Red Scare period (1946-1956), all manner of covert operations were implemented to uncover Communist sympathisers and those perceived to be unloyal.

The Trump ‘tweets’ seem linked to an alleged order sent by the Foreign Intelligence Surveillance Court instructing surveillance on suspected liaisons between Mr Trump, some of his associates and a number of Russians. As yet, no documentation has surfaced confirming such an order was ever given.

Intelligence officials in the USA described the allegations as “simply false.” Intelligence sources told Eye Spy that official electronic surveillance (including physical wire-tapping) could only have taken place with a warrant. “That warrant can only be issued by the Foreign Intelligence Surveillance Court on the premiss that Trump had committed a federal crime or was acting as a foreign spy. And that’s highly unlikely.”



US and UK Intelligence reject claims of ‘wiretapping’ and ‘eavesdropping’ at Trump Tower in New York

Continued on page 82



VOLUME 2
VOLUME 3
VOLUME 4
VOLUME 5
VOLUME 6
VOLUME 7
VOLUME 8

ORDER ON-LINE www.eyespymag.com OR USE ORDER FORM ON PAGE 82

VOLUME 9



ISSUE 65 REF: ES/65
UK £3.95 USA ROW \$7.00



ISSUE 66 REF: ES/66
UK £3.95 USA ROW \$7.00



ISSUE 67 REF: ES/67
UK £3.95 USA ROW \$7.00



ISSUE 68 REF: ES/68
UK £3.95 USA ROW \$7.00



ISSUE 69 REF: ES/69
UK £3.95 USA ROW \$7.00



ISSUE 70 REF: ES/70
UK £3.95 USA ROW \$7.00



ISSUE 71 REF: ES/71
UK £3.95 USA ROW \$7.00



ISSUE 72 REF: ES/72
UK £3.95 USA ROW \$7.00

VOLUME 10



ISSUE 73 REF: ES/73
UK £3.95 USA ROW \$7.00



ISSUE 74 REF: ES/74
UK £3.95 USA ROW \$7.00



ISSUE 75 REF: ES/75
UK £3.95 USA ROW \$7.00



ISSUE 76 REF: ES/76
UK £3.95 USA ROW \$7.00



ISSUE 77 REF: ES/77
UK £3.95 USA ROW \$7.00



ISSUE 78 REF: ES/78
UK £3.95 USA ROW \$7.00



ISSUE 79 REF: ES/79
UK £3.95 USA ROW \$7.00



ISSUE 80 REF: ES/80
UK £3.95 USA ROW \$7.00

VOLUME 11



ISSUE 81 REF: ES/81
UK £3.95 USA ROW \$7.00



ISSUE 82 REF: ES/82
UK £3.95 USA ROW \$7.00



ISSUE 83 REF: ES/83
UK £3.95 USA ROW \$7.00



ISSUE 84 REF: ES/84
UK £3.95 USA ROW \$7.00



ISSUE 85 REF: ES/85
UK £3.95 USA ROW \$7.00



ISSUE 86 REF: ES/86
UK £3.95 USA ROW \$7.00



ISSUE 87 REF: ES/87
UK £3.95 USA ROW \$7.00



ISSUE 88 REF: ES/88
UK £3.95 USA ROW \$7.00

VOLUME 12



ISSUE 89 REF: ES/89
UK £3.95 USA ROW \$7.00



ISSUE 90 REF: ES/90
UK £3.95 USA ROW \$7.00



ISSUE 91 REF: ES/91
UK £3.95 USA ROW \$7.00



ISSUE 92 REF: ES/92
UK £3.95 USA ROW \$7.00



ISSUE 93 REF: ES/93
UK £3.95 USA ROW \$7.00



ISSUE 94 REF: ES/94
UK £3.95 USA ROW \$7.00



ISSUE 95 REF: ES/95
UK £3.95 USA ROW \$7.00



ISSUE 96 REF: ES/96
UK £3.95 USA ROW \$7.00

VOLUME 13



ISSUE 97 REF: ES/97
UK £3.95 USA ROW \$7.00



ISSUE 98 REF: ES/98
UK £3.95 USA ROW \$7.00



ISSUE 99 REF: ES/99
UK £3.95 USA ROW \$7.00



ISSUE 100 REF: ES/100
UK £3.95 USA ROW \$7.00



ISSUE 101 REF: ES/101
UK £3.95 USA ROW \$7.00



ISSUE 102 REF: ES/102
UK £3.95 USA ROW \$7.00



ISSUE 103 REF: ES/103
UK £3.95 USA ROW \$7.00



ISSUE 104 REF: ES/104
UK £3.95 USA ROW \$7.00

VOLUME 14



ISSUE 105 REF: ES/105
UK £3.95 USA ROW \$7.00



ISSUE 106 REF: ES/106
UK £3.95 USA ROW \$7.00



ISSUE 107 REF: ES/107
UK £3.95 USA ROW \$7.00

EYE SPY INTELLIGENCE MAGAZINE **YOUR BRIDGE TO THE COVERT** **WORLD OF ESPIONAGE**

EYE SPY 16 YEARS OF PRODUCTION!

Each highly collectable edition represents a worldwide overview of global intel events and covers every aspect of the subject's astonishing **SPY TRADECRAFT...**

• PRICE INCLUDES POSTAGE AND PACKING • ORDERS SENT AIRMAIL

ORDER BY TELEPHONE: UK, EUROPE/WORLDWIDE + (0)1756 770199 (UK) NORTH AMERICAN READERS TOLL FREE: 877 309 9243

Stocks are now running low on several editions... secure these valuable print copies now!

AIR

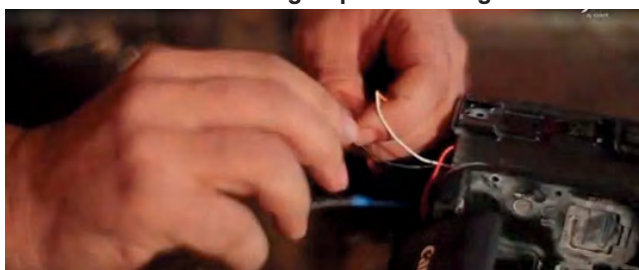
DECEPTION

**POPULAR ELECTRONIC MEDIA
BANNED ON CERTAIN AIR ROUTES**

CIA and MI6 analysts combine various intelligence reports and issue 'clear and present danger' warning to US and UK intelligence services



Ibrahim al-Asiri teaches his bomb-making skills to several terrorist groups - including ISIS



On receipt of intelligence gleaned from overseas agents, US officials moved quickly to introduce new

airflight security measures. Larger electronic devices such as laptops, iPads and cameras will no longer be allowed as carry on baggage for direct flights from certain Middle East and North African nations. Items included in the ban are

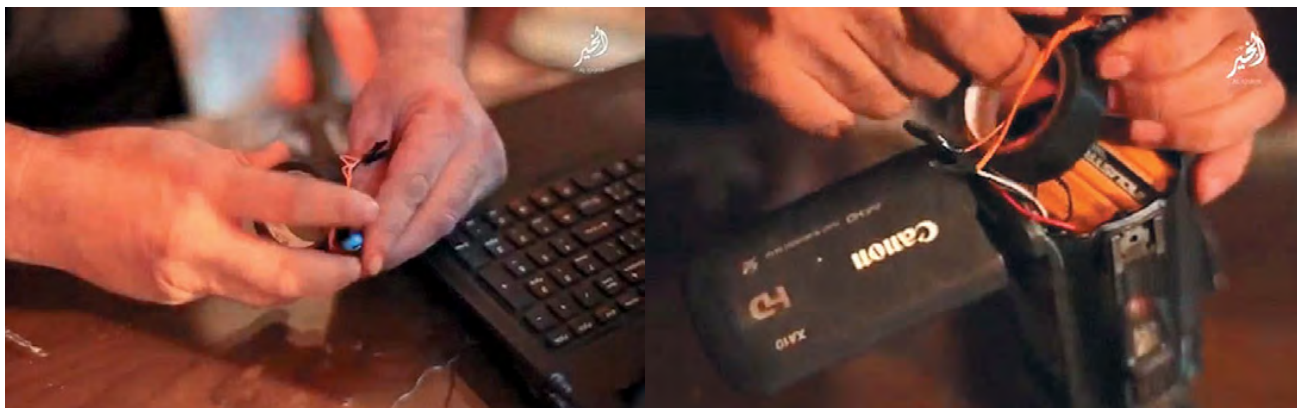
laptops, tablets, e-readers, cameras, portable DVD players, electronic game units larger than a smartphone and travel printers/scanners. Within 24-hours, the UK adopted similar measures but with slight differences: the US ban applies to 10 airports in the Middle East including, Morocco, Turkey, Saudi Arabia, Jordan, Kuwait, Qatar and Egypt. Britain's restrictions apply to flights originating from Turkey, Lebanon, Jordan, Egypt, Tunisia and Saudi Arabia.



Intelligence sources told Eye Spy the counter-measures are almost certainly related to Ibrahim al-Asiri, al-Qaida's master bombmaker who now operates on behalf of ISIS and other terrorist outfits. There is also some evidence to suggest materials were secured after a raid against al-Qaida positions in Yemen in January. During this operation, US Navy SEAL Ryan Owens was fatally wounded.

For the best part of a decade, the CIA has searched for al-Asiri, who has 'peddled' his enhanced bombmaking skills to numerous groups and individuals in the Arabian Peninsula. Many of his new bombs combine explosives with electronic technology - some of which have already been tested. The recent release of an appalling video by ISIS is





These stills from a 2016 ISIS video show the construction of a laptop bomb (left) and a camera bomb. Intelligence gleaned from various sources, including materials from informants in Mosul led to the ban

evidence enough that he has managed to create working bombs hidden in small devices such as laptops and cameras. Similarly, two years ago he boasted that he would soon have a bomb that would be able to defeat airport security measures.

For the record, the June 2016 ISIS video showed several journalists who were blown-up by camera and laptop bombs detonated around their necks.

Al-Shabaab, the al-Qaida franchise whom al-Asiri has provided guidance, claimed responsibility for the 2 February 2016 explosion on board Somalia Daallo Airlines Flight 159. In this case a bomb hidden in a laptop blew a hole in the fuselage.

Ibrahim al-Asiri, born in Saudi Arabia, has a lengthy crime sheet. The CIA believe he is directly linked to several high-profile terrorist attacks, many involving the aviation industry.

A TRAIL OF DESTRUCTION

- August 2009. Built the device used by his brother Abdullah al-Asiri in the suicide bombing of the Jeddah office of security chief Mohammed bin Nayef, using a PETN bomb hidden in his rectum.

- The Christmas Day underwear bomb plot 2009. In this case al-Asiri concealed a device in underwear worn by al-Qaida operative Umar



Umar Farouk Abdulmutallab - the 'underpants bomber'



2016. Explosives detonated in a laptop caused this damage to Daallo Airlines Flight 159



Eric Swalwell

Farouk Abdulmutallab on a flight Amsterdam to Detroit. The detonator failed to ignite the explosives.

- 2010. The cargo plane bomb plot. Plastic explosives were found on separate cargo aeroplanes flying from Yemen to the United States. Plot uncovered by UAE security services. Devices concealed in ink jet cartridges.

- The crash of UPS Flight 6 flying between Dubai International Airport and Cologne Bonn Airport. A fire caused by the autoignition of the contents of a cargo pallet containing "a significant number" of lithium type batteries and "other combustible materials."

- May 2014. MI6 secure intelligence on al-Asiri regarding liquid explosive implants. (See Eye Spy 92)

- May 2016. Somali security forces foil ISIS attack in Mogadishu. A vehicle and seven laptops reportedly adapted for carrying explosives are recovered.

US House Intelligence Committee member Eric Swalwell commented on the new security measures. "There was 'a new aviation threat. We know that our adversaries, terrorist groups both in and out of the United States are seeking to bring down a US-bound airliner. That's one of their highest value targets. And we're doing everything we can right now to prevent that from happening."

Sceptics say the devices could explode in checked luggage. "And what if the carrier takes a connecting flight," one security analyst said.

US intelligence specialists told Eye Spy all the evidence suggests that at this moment the laptop bombs would need to be manually triggered. Of relevance also, the detonator seems to be linked with the battery.

The ban is already in place.

**FROM FRESH
NEWSPAPERS TO
ALL NEW MUSIC RELEASES**

ONLY ON

AVXHOME.IN



**OUR SEARCH SITE HELPS
TO FIND ALL YOUR
FAVOURITE MAGAZINES**

SOEK.IN

**JOIN US ON
FACEBOOK**

MCGUINNESS

IRA Commander Turned Peacemaker

Martin McGuinness, 66, former IRA Chief of Staff and central figure in the Northern Ireland peace process, has died after a short illness, just two months after stepping down as Northern Ireland's Deputy First Minister.

Reactions to his death have been mixed. To many he was a peacemaker who played a key role in ending the violence - better known as 'The Troubles' - in which nearly 2,000 people died. Close friend and colleague Sinn Féin President Gerry Adams said: "Throughout his life Martin showed great determination, dignity and humility and it was no different during his short illness." Others still refer to him as a "hardened terrorist."

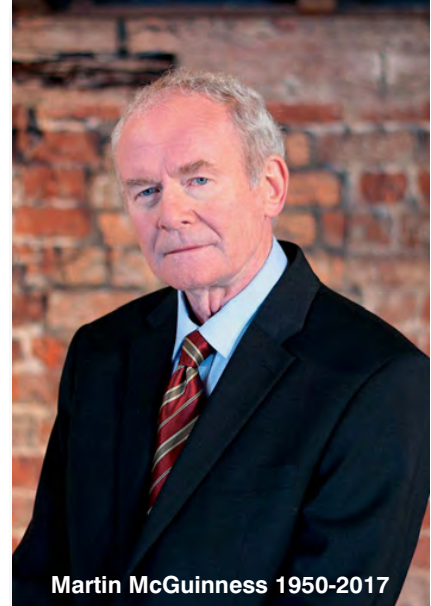
Prime Minister Theresa May said of McGuinness: "While I can never condone the path he took in the earlier part of his life, Martin McGuinness ultimately played a defining role in leading the Republican movement away from violence. In doing so, he made an essential and historic contribution to the extraordinary journey of Northern Ireland from conflict to peace."

Former Prime Minister Tony Blair who orchestrated the Good Friday Agreement negotiations concluded in 1998, said: "Whatever the past of Martin McGuinness, I don't think it's inappropriate, in fact I think it's absolutely right today at this moment of his passing, to remember what he did for peace,



what he did for the island of Ireland in resolving one of the great conflicts in the world."

Such viewpoints are not held by Lord Tebbit, a former Chairman of the Conservative Party, who was in Brighton's Grand Hotel when the IRA bombed the building in 1984. It was an audacious attempt to assassinate Prime Minister Margaret Thatcher. Five people were killed in the attack, which also seriously injured his wife Margaret. "It's not merely that

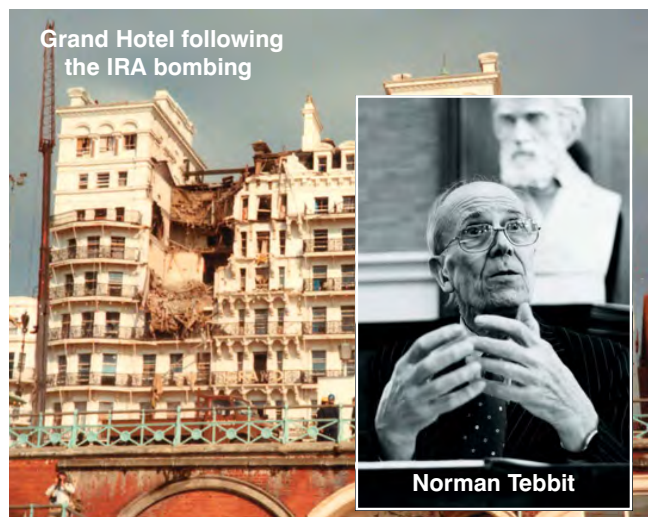


these creatures [the Brighton bombers] crippled my wife, but they also murdered five of my friends. I only hope that his death will help to bring some sort of closure to those families and friends of whose murder he's accomplished." He added: "He was a coward."

Tony Blair's former adviser Alastair Campbell, was also involved in the Good Friday talks. He said: "Of course his terrorist past is a big part of his story. But so is the choice he made to leave it behind."



2014. An historic moment as Martin McGuinness meets HM The Queen at Hillsborough Castle, Northern Ireland



ALTERNATIVE HACKING



Case files which show the good, bad, fascinating and ugly side of operational interference



Hacking, cyber espionage, cyber warfare and cyber security dominate the headlines of today. Most people associate these subjects with the Internet and the explosion of technology used in every aspect of our lives. Warning of their potential damage is now fairly standard government procedure. However, used in the context of intelligence, such terminology carries a broader meaning and historically has had major implications for nation states and the public alike.

Very few people realise that the first 'hackers' started centuries ago. Individuals or groups assessing their own resiliency to attack; revealing vulnerabilities and alerting them to the consequences of exploitation more than 1,500 years ago. Today, the intelligence world calls this Process Managed Security (PMS) - testing or penetration - ethical hacking.

Our hacking ancestors actually originated in ancient India after a strategy game known as Chaturanga was invented. Point and counter point skirmishing through board games began in the 6th century and eventually evolved into Chess. Here 'battle-hardened' tacticians honed their skills by anticipating opposition strategy, feints or moves. There were also references to



military 'tiger teams' - a term which would be used again in the 20th century in connection with hacking, systems and facility testing, security procedures and counter-espionage.

All these historical points in time would eventually, when technology advanced, become integral in today's computer operating systems and applications.

THE ROGUE OPERATORS

Perhaps the earliest known incident of modern technological 'mischief' can be traced back to 1878 and the fledgling days of the Bell Telephone Company. Here teenage boys hired by Bell as switchboard operators, intentionally misdirected and disconnected telephone calls, eavesdropped on conversations and played



Boys operating telephone switches

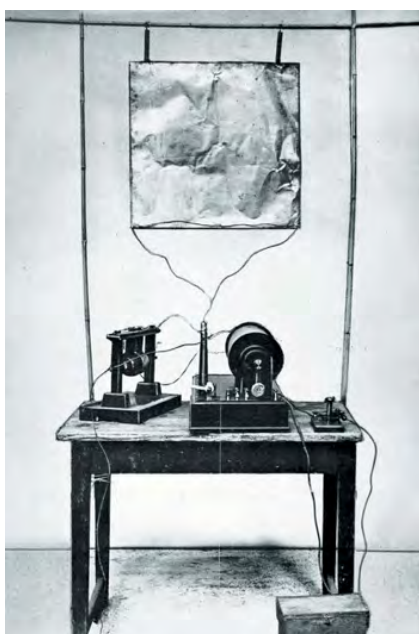
© THE TELECOMMUNICATIONS HISTORY GROUP



Guglielmo Marconi as depicted by Spy in *Vanity Fair* in 1905. The caption reads - 'Wires without wires'



Marconi with his long-distance radio transmission system



Recreation of Marconi's first transmitter built in 1895



a variety of other pranks on unsuspecting customers. Bell's chief engineer referred to the boys as 'Wild Indians', and is at least one reason why the company opted to recruit an all-female operator workforce and introduce new security regulations.

MARCONI AND INTERCEPTION

Communication and signals play an integral part in the way intelligence, military and government officials help provide security. However, all are prone to interception. One famous Italian physicist, who could testify to such an act is Guglielmo Marconi. He developed a wireless telegraph in the early 1900s in which he believed he could broadcast safe radio-telegraphic messages on a specific wavelength. In essence, a two-way invisible communication channel safe from would-be eavesdroppers.

Marconi was up against several inventors and already functioning and emerging wired-telegraph companies. None was more powerful, however, than the Eastern Telegraph Company (ETC). Marconi's work was perceived as a direct threat, and thus they sought to dampen enthusiasm for his 'unbreakable wireless technology'. The ETC turned to an unlikely man for help - magician and inventor in the person of John Nevil Maskelyne. Like Marconi, he too had engaged and experimented with wireless technologies. Maskelyne cleverly built broadband receivers which could intercept Marconi's transmissions and a plan was hatched.

By 1903, and with a fascinated global audience, Marconi prepared to demonstrate his system in London. He had arranged to receive a message from over 300 miles away.

However, quite unexpectedly, a message was received, but not the one Marconi had been waiting for - and this one arrived early. *'Rats rats rats rats... There was a young fellow of Italy... who diddle the public quite prettily'*. Other derogatory remarks followed.

An infuriated Marconi wrote to the *Times of London*, describing the perpetrator of the breach as a '*scientific hooligan*', he asked readers to help find the culprit. He did not, however, have long to find out. Maskelyne himself wrote to the newspaper and confessed he had performed the act to demonstrate security flaws in Marconi's invention. Maskelyne pointed out that if it was possible to send a message to Marconi's receiver, then it was just as likely messages could be intercepted.



John Nevil Maskelyne



Map showing Eastern Telegraph Company global network in 1901



Blue box unit used by phreakers to engage telephone systems

PHREAKERS

When electronic telephone switching networks emerged in the late 1960s, it didn't take long for some shadowy characters known as 'phreakers' to circumnavigate the system allowing people to make expensive long distance phone calls free of charge.

How this was achieved is fascinating. Phreakers called the telephone exchanges listening and recording sounds - tones, clicks, clunks, beeps etc. to try and understand the mechanism of how calls were routed. Armed with technical journals to educate themselves and often visiting exchanges and 'dumpster diving' - removing notes and papers from rubbish bins - they soon discovered how to trick the automated systems.

To discover more secrets they would often call the operators pretending to be telephone company engineers - thus securing more

answers. However, the phreakers went further, and at night entered exchanges and attached custom-built boxes with a mechanism that attached itself to the system. The units, called blue boxes, basically allowed phreakers to make free calls.

As the months went by, the tricks of the trade were passed to friends and associates, and soon the FBI became involved. Arrests followed and a number of people were jailed. It was a complex business, but the phreakers essentially used the system believing it was a free and harmless resource. It has also been alleged, that some well known computer figures actually sold the phreaking machines to raise finance!

The culture of phreaking ended in the 1980s, when telephone exchanges were automated and computer controlled. Yet there is a legacy. Illegally entering computer systems or similar electronic media is occasionally referred to as

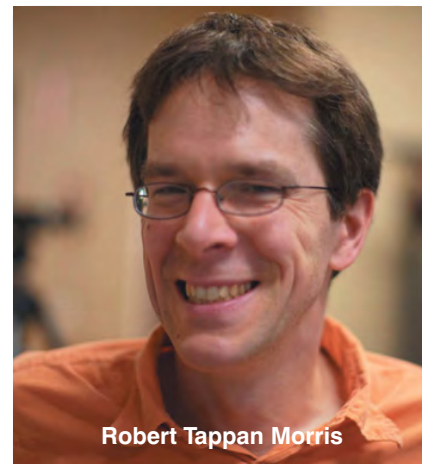
the 'HP culture'. In this case the H standing for hacking and the P for phreakers or phreaking.

MORRIS WORM

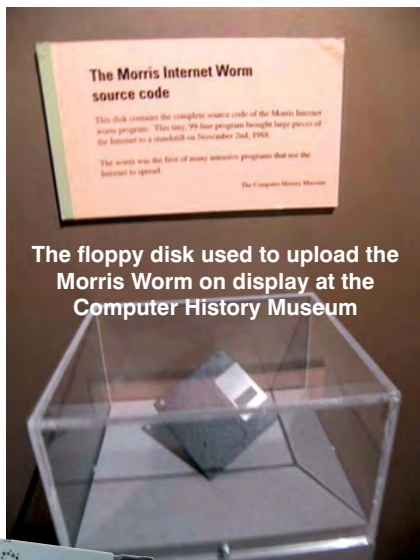
Much has been written about computer viruses and the impact they can have on all manner of systems, from closing down power plants and banks to damaging entire global communication networks. It is not a new phenomenon, the first publicised attack occurred almost three decades ago, and spread through an emerging Internet.

Cornell University graduate, Robert Tappan Morris, 23, created the first recognised 'computer worm' which he uploaded from a computer at Boston MIT - this to help conceal the fact that it was written at Cornell. The malware replicated itself and spread to computer systems across the United States; universities, military facilities and a number of important research and test centres were all affected. Machines would slow and eventually stopped working altogether. FBI investigators later revealed the virus had infected around 6,000 machines connected to the Internet. At this time the figure represented an astonishing 10% of all computers. It was an attack ➤

John Draper - a former phreaker and computer programmer who is well known amongst today's hacking and security community



Robert Tappan Morris



The floppy disk used to upload the Morris Worm on display at the Computer History Museum



The caption reads: 'This disk contains the complete source code of the Morris Internet worm programme. This tiny, 99-line programme brought large pieces of the Internet to a standstill on November 2nd, 1998'

that the Bureau estimated cost the country \$10 million.

However, there was an inadvertent upside to Morris's action. The Defense Advanced Research Projects Agency (DARPA), decided to allot monies to help finance the creation of CERT, a specialist computer emergency response organisation that would tackle future cyber breaches and incidents. CERT was based at Carnegie Mellon University, Pittsburgh, and could be described as America's first authentic, though civilian-operated 'cyber command'.

As for Morris, besides his claim to fame as the creator of the first 'computer worm', he also became the first person to be convicted and fined under the Computer Fraud and Abuse Act.

Putting his past shadowy work behind him, Morris co-founded Viaweb. And in 2005, sold the company to Yahoo for nearly \$50 million. Today he is a professor of electrical engineering and computer science at MIT.

A HONOURABLE ENDEAVOUR

During WWII, many inmates and workers used by the Nazis to build munitions, deliberately sabotaged

war-related materials, including rockets and missiles, in order that they malfunctioned. Yet the actions and work of one man, engaged in another type of sabotage, could be described as 'computer hacking'.

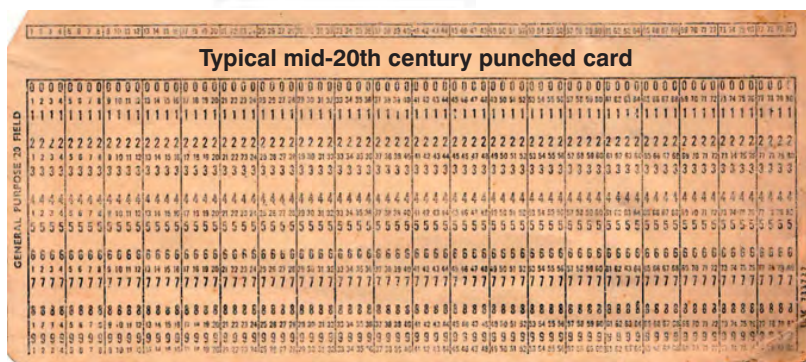
When Germany overran France, Berlin moved quickly to identify residents and all those perceived as enemies of the state. One of the first tasks of the pro-Nazi Vichy government was a nationwide census. As well as ascertaining jobs, family members, etc., people were asked to reveal their religion and creed. This spelt a problem for Jewish citizens. One man engaged in the identification process was Rene Carmille. He was a skilled punched card computer expert and comptroller general of the French Army in 1940. Carmille headed the Demographics Department of Vichy and the soon-to-be created INSEE, (National Statistics Service), operating information-processing machines which read census cards. The organisation was large, employing around 2,000 people.

Unbeknown to the Germans, he was also a member the French Resistance element known as the Marco Polo Network. Carmille asked Berlin for the post of overseeing personal information from the census forms onto tabulator cards, which could then be read and analysed. One section on the card was called 'Column 11'. This was where data on religion was flagged allowing the Nazis to detain Jewish people, many of whom were already being sent to concentration camps.

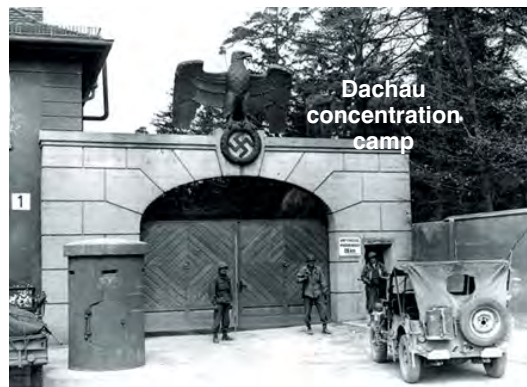


Rene Carmille

Carmille deliberately stalled the process and intentionally reprogrammed the card readers thus circumnavigating Column 11. This meant no detail would be displayed on the card.



Typical mid-20th century punched card



Dachau concentration camp



Klaus Barbie

Similarly, Carmille and close associates sifted through the census forms and cards to find people who were anti-Nazi and likely to join the Resistance.

Carmille's 'ethical hacking' project continued, but he was finally arrested in Lyon in early 1944. Despite being tortured and interrogated by the notorious Klaus Barbie, he maintained his silence. Sadly he died just five months before the end of the war at the Dachau concentration camp. His brave actions, however, saved countless lives.

SUMMARY

Hacking and its related fields have existed for centuries, but today use of the term 'ethical hacker' and its meaning is very much dependant upon a person's point of view. Edward Snowden is a good example. He has support from those who object to 'big brother' and global surveillance, whilst he is scalded a villain and spy for revealing details of programmes which are defensive and related to national security.

Few would object to the actions of Rene Carmille. Nor was there any dissenting voice when the NSA (CIA-backed) interfered with ISIS propaganda videos. Ethical hacking is an emotive term which has divided opinion for decades. Incidents will undoubtedly continue, but like the description and meaning of Intelligence, it is a subject immense in size and swollen further by a variety of complex and controversial attachments.

TIGER TEAMS

Games, training, testing security, penetration, counter-measures, espionage and vulnerabilities

1812. Lieutenant Georg Leopold von Reisswitz developed 'Kriegsspiel' - a war game used for training officers in the Prussian and German armies (tactics and manoeuvres).



1889. The US Navy adopts war-gaming as a training tool through military simulation.

1964-2017. Tiger Team. A phrase commonly used to describe a collection of experts assigned to investigate, solve, build, or recommend possible solutions to unique problems. In one mid-1960s project such a team was asked to test computer security used by NASA and the American military.

Tiger Teams have also been used in counter-espionage and exercises testing base security. Units are directed to

breach (test) restricted areas, secure stored and guarded documentation and determine just how easy it is to deposit or remove explosives etc. Such covert actions have

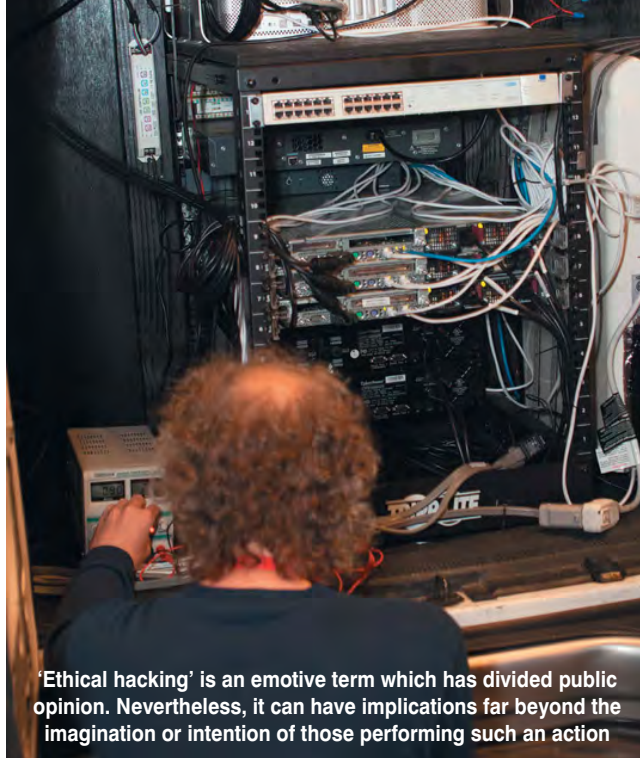
been likened to hackers who engage military and government computer systems in an effort to circumnavigate security barriers. Indeed, today the NSA operate its own Cyber Defense - appropriately called Tiger Team (Red Cell).

1974. The US Air Force conducts its first ethical hack - a security evaluation of the Multics operating system.

1984. US Navy Commander Richard Marcinko builds and leads a team of SEALs to test naval bases vulnerability to terrorism (Red Cell or Tiger



Tiger Teams continue to operate today in many fields including cyber



'Ethical hacking' is an emotive term which has divided public opinion. Nevertheless, it can have implications far beyond the imagination or intention of those performing such an action

Team). A more formal identification name is National Security Co-ordination Team (NSCT).



Richard Marcinko

1989. The US Department of Energy introduce Tiger Teams to test and access DOE facilities regarding safety,



John Patrick

Teams still occasionally operate on behalf of the DOE today.

1995. IBM's John Patrick coins the term ethical hacking

environment and health subjects. The project lasted three years. Tiger



2016 International Conference on Cyber Security, New York City

A Matter of Assu

© NEW SCOTLAND YARD/CROWN COPYRIGHT



Just days before a terrorist attacked in central London, counter terrorism operation played out on River Thames

Pleasure cruisers, cargo ships and other vessels are a regular sight on the River Thames in London. With this in mind, hijacking and water-borne attack scenarios are not lost on the protectors of London and other cities. A decade ago, al-Qaida planned to hijack and explode large vessels carrying fuel and liquid gas traversing the eastern seaboard of the United States. This prompted the US authorities to introduce new security measures. And today, counter-terrorism exercises regularly take place at inland ports and cargo facilities.

To examine how London would respond to an actual terror attack on water, New Scotland Yard, MI5, Special Boat Service (SBS) and other emergency forces played out a realistic hijacking of a tourist vessel by terrorists on the river in March. The exercise, codenamed Operation Anchor, involved around 200 officers and six 'terrorists'. The Port of London Authority, Maritime and Coastguard Agency, RNLI, London Fire Brigade and London Ambulance Service all participated.

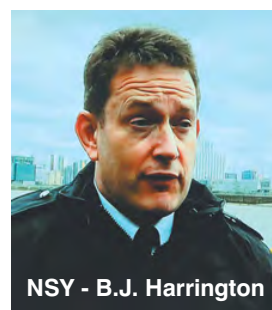
The media were invited to observe two fast police boats race to board a City Cruises boat



Playing the part - an armed 'terrorist' on the cruise boat

where dozens of people had been taken hostage by armed gunmen. The situation was diffused, but in reality, no one can predict the outcome or actions of a suicidal bunch of terrorists. Ultimately, the operation was one of public assurance and forces preparedness.

Whilst NSY was keen to state the exercise was not the result of any immediate threat to the maritime industry, the fear of such a happening is very real. Armed undercover officers are now deployed on cross channel ferries, and similar details are based at several major ports. Officials are also in constant discussion with ferry and passenger lines regarding intelligence on possible terrorist attacks and the movement of terrorists, firearms and explosives.



NSY - B.J. Harrington

Commenting on the London exercise, New Scotland Yard Commander B. J. Harrington, said: "Exercises such as this one show that London is prepared and should reassure anyone who lives, works or visits London that there is an amazing team of highly dedicated, professional and skilled men and women

Iran



© NEW SCOTLAND YARD/CROWN COPYRIGHT



ready to keep them safe from this kind of threat.”

SHOPPING CENTRES ON ALERT

Al-Qaida and now ISIS, endorses and encourages its members to strike soft targets such as shopping centres. With limited protective security measures, the potential for

mass casualties is obvious. In recent years, attacks at popular locations frequented by large numbers of people have increased.

Britain's National Counter Terrorism Security Office (NaCTSO) holds training days for shopping centres and other vulnerable targets around the country. An official said: “Terrorist attacks in the UK are a real and serious

CT exercise Canary Wharf, London 2016

danger. Crowded places, including shopping centres, are likely to feature in the attack plans of terrorist organisations in the future.”

Training and security operations are now a familiar sight in Britain's major cities.

The fear amongst senior CT officials is complacency. And, as ISIS fighters return to their home countries in Europe and elsewhere, the risk of an attack on land, sea or in the air increases daily.



CT officers board the cruise boat

UNATTENDED ITEMS: LOST... or SUSPICIOUS?



H

Hidden?

- Has it been concealed or hidden from view?
- Bombs are unlikely to be left in locations such as this – where any unattended item will be noticed quickly.



O

Obviously suspicious?

- Does it have wires, circuit boards, batteries, tape or putty-like substances?
- Do you think the item poses an immediate threat to life?



T

Typical?

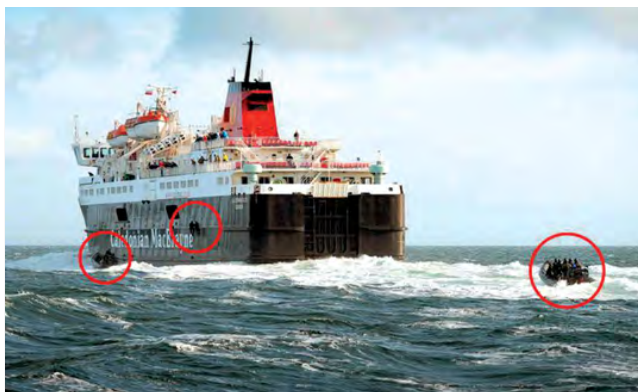
- Is the item typical of what you would expect to find in this location?
- Most lost property is found in locations where people congregate.

If after applying the HOT protocols you still believe the item to be suspicious, call 999.

NaCTSO
National Counter Terrorism Security Office



2015. Royal Navy Marines personnel (43 Commando Fleet Protection Group) in a simulated ferry hijacking exercise



© MINISTRY OF DEFENCE/CROWN COPYRIGHT

CI



TRADECRAFT

THE SECRET WORLD OF

BY DR CHRIS NORTHCOTT

Part 4

COUNTERINTELLIGENCE

COUNTER-INTELLIGENCE ANALYSIS

As the foregoing analysis of deception and double-agents has shown in the last feature, safeguarding one's own intelligence operations can be very complicated indeed - it entails much more than simply detecting the occasional spy.

Cases may often be connected to each other. Thus, the overall mission of protecting one's own intelligence community against deception and penetration necessitates a dedicated unit focused upon counter-intelligence analysis, in order to function as an institutional memory and to assess these links between cases. Probably the best way to decide if one's own intelligence community has been infiltrated is to recruit a high-level agent inside the hostile intelligence service (either an agent-in-place

or a defector). However, even in these circumstances, it would be quite unlikely that the source would be able to provide the actual names of the spies working for his side. The source would probably only be able to name these spies if the source was directly employed in running them, or if he was a very senior officer of the hostile intelligence service. It is much more likely that the source would only be able to offer clues to these spies' identities.

SINGLE AGENT SOURCING

Much analysis would be required to obtain results from such leads. For example, one may receive intelligence that a hostile intelligence service has gained access to a few classified documents on a particular subject. If they had all been provided by the same agent, one could analyse the distribution lists of these documents in order to determine



who had access to every one of them. The source may reveal that the spy had a meeting with his controller in a specific foreign city on a certain date. Analysing travel records would show which officials with access to the leaked information were in that city on that date. There may be other clues which point to other kinds of penetration by a hostile intelligence service. For example, if an operation fails, or a



FBI analysts attend a briefing



View from inside the Pentagon following the 9/11 attack

The work of a counter-intelligence organisation relies on input from numerous sources and agencies. Though still the leading edge in countering espionage and subversive acts, much of the work conducted by domestic intelligence agencies engaged in counter-intelligence, now focuses on terrorism and wider national security threats, including financial, cyber and commercial

technical collection system is detected or an agent is arrested, in a manner which suggests that the hostile intelligence service had learned about this operation before it happened. An investigation is required to determine how the adversary might have discovered this operation. There will probably be many possible avenues by which this information could have fallen into the hands of the foreign intelligence service - such as security lapses and vulnerabilities, or people with access to this information. However, if there is a spate of such breaches, it may well be possible to narrow down the options. For example, maybe only one particular official had access to all of

the leaked information. In any case, a series of such intelligence breaches should draw an intelligence service's attention to the possibility that a hostile intelligence service has effective technical or HUMINT intelligence gathering capabilities that need to be detected and neutralised.

SECURITY STRUCTURES

Responsibility for information security became institutionalised in the West, like intelligence, during the Victorian era. Military Intelligence departments were made responsible for security in the field and providing ciphers. The



threat from German espionage led to the foundation of the British Secret Service Bureau (SSB) in 1909. The First and Second World Wars and Communism had great impacts upon the developments in security, as with intelligence. Like intelligence, it was slowly learned that information security required an inter-departmental coordination of measures. A defensive information security community reflected the way in which offensive intelligence collection worked across the boundaries of targets and techniques. The Cold War taught the West that little was gained by investing in high-quality ciphers if Soviet Intelligence was able to recruit cipher clerks who could provide them with copies of these ciphers.

Complementary intelligence collection attacks have a synergy. Therefore, the defence requires a like capability to integrate security across organisational boundaries. During the Second World War, the British established the Security Executive and an inter-departmental security structure alongside and linked to





AWAY DAYS:

Today, counter-intelligence officers operate in all fields of the intelligence cycle. Here two US officers drive through the streets of Kabul, Afghanistan

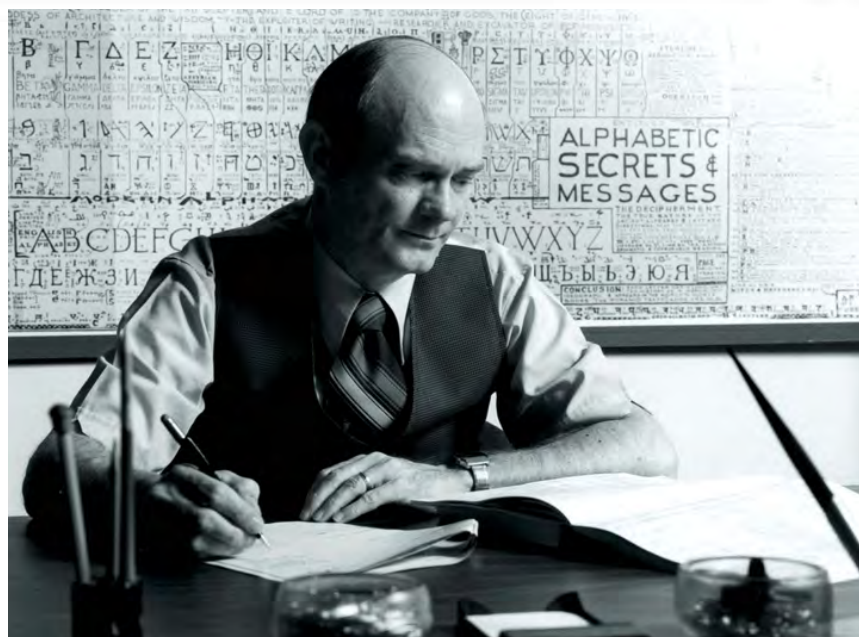
the Joint Intelligence Committee (JIC) and the control of strategic deception. In the 1980s, the USA developed the concept of Opsec, all-source operational security embracing the complete spectrum of defensive measures. Governments require organised security policies and actions and intelligence makes its inputs to them. In this sense, the security authorities are intelligence's customers. In addition, one of the components of information security is intelligence's own protection. In this regard, intelligence is also one of its own customers.

It is instructive to now look at the particular contributions that the intelligence community makes to information security.

THREAT ASSESSMENTS FOR DEFENSIVE SECURITY MEASURES

Security should be based upon intelligence assessment. Intelligence threats from other states are evaluated on evidence regarding their foreign intelligence services that has been provided by counter-intelligence (intelligence on foreign intelligence).

Not surprisingly, foreign intelligence services tend to be the most security-conscious of all of intelligence's targets. Therefore, it is extremely difficult to mount intelligence attacks upon them. IMINT (Imagery Intelligence) may provide some information on external facilities, like foreign intercept bases, but not on their activities and successes. SIGINT (Signals Intelligence) on foreign intelligence communications has the potential to provide vital insights - as shown by British penetration of German Abwehr ciphers during WWII. Discovery of an adversary's technical



Cold War Agenda. An FBI cryptologist seeks to break a secret code. Note the fascinating board behind the codebreaker

equipment for bugging and eavesdropping provides some idea of their capabilities. However, the primary sources on intelligence threats tend to be the infrequent HUMINT (Human Intelligence) ones - intelligence officers recruited inside foreign intelligence services and defectors. Thus, assessments of intelligence threats are usually composed from scraps of technical intelligence collection and rare windfalls from HUMINT.

The comprehensive study of foreign intelligence is hard work and has raised concerns regarding devoted resources. During the Cold War, counter-espionage and counter-intelligence against Soviet HUMINT were

considered extremely important. However, coverage of other Soviet intelligence was a lesser priority. For example, it was unclear how necessary it was to know exactly what Soviet IMINT satellites could photograph and whose role it was to assess this. Threat assessments can become reflections of the offensive capabilities of one's own side. For example, as the West was not at first skilled in close-range eavesdropping, it took a while to appreciate the degree of Soviet bugging of Western embassies in Moscow during the 1940s and 1950s. At other times, a 'worst case' assessment of Soviet threats was put forward in order to make governments more security conscious. This kind of exaggeration



Cold War Days. FBI employees relate messages on teletype machines

influenced US assessments of the threat posed by the USSR's push to acquire Western technology.

Nevertheless, despite the problems of producing accurate intelligence threat assessments, reasonable security policies begin from them. This involves specific details not just general capabilities. For example, Western security in the Cold War regarding testing new electronic emissions relied upon precise evaluations of how far they could be intercepted by the USSR's SIGINT ships skirting the coasts of NATO countries. And, for the purposes of personnel security vetting against ideological espionage, somebody has to evaluate what the ideological threats are and who may try to take advantage of them.

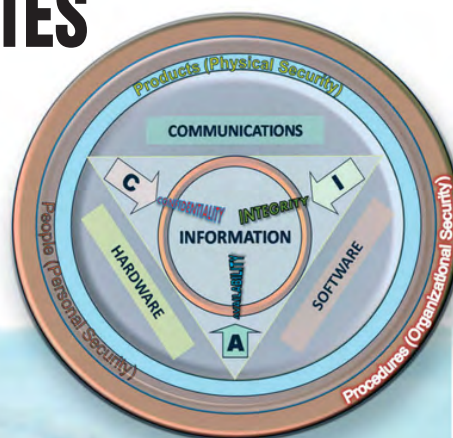
COUNTER-ESPIONAGE

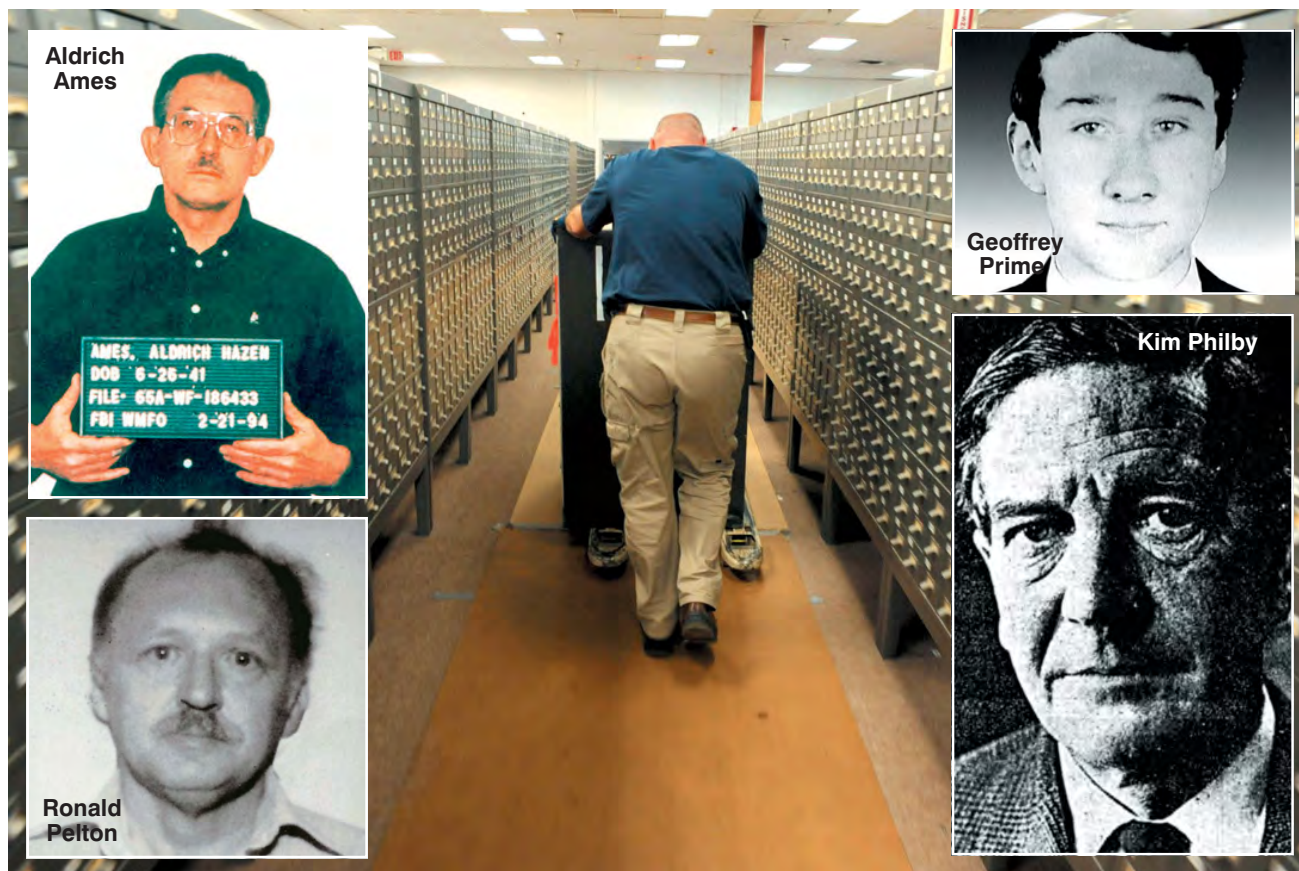
Counter-espionage's detection and neutralisation of foreign espionage is the largest effort focused on direct action against foreign intelligence threats. As a part of security intelligence, counter-espionage is in distinct ways different from the main intelligence system. Counter-espionage is primarily

INFORMATION SECURITY ATTRIBUTES



Information systems are composed of various elements, topics, subjects, etc. and are governed by both physical and human attributes. A breach in any component in the world of intelligence could lead to compromise, a loss of information and have serious implications for national security





Information security is an integral part of counter-intelligence work. However, despite the best endeavours of many agencies and strict control of how such material is handled, information and secrets will forever remain vulnerable to exposure through espionage, as these four US-UK intelligence officers and KGB agents proved

oriented to detection; whereas foreign intelligence's quest is for broader understanding. In this sense, counter-espionage should be perceived as a discrete contribution to information security. However, this is not the complete picture. Firstly, counter-espionage handles only one type of intelligence threat - HUMINT, and not SIGINT or IMINT. Secondly, there is a close link between a state's counter-espionage and counter-intelligence organisations. Counter-espionage discovers and neutralises individual cases of espionage, which can offer leads back into the foreign intelligence organisation handling those agents. And, counter-intelligence's infiltration of intelligence opponents can give leads for counter-espionage. Therefore, regardless of its institutional separation, counter-espionage is firmly linked to counter-intelligence's work to infiltrate the adversary's intelligence system, negate its successes and even exploit them through deception.

PENETRATING FOREIGN INTELLIGENCE

Counter-intelligence (in the wide sense of intelligence on foreign intelligence) does more than just give evidence for threat assessments. Successful counter-intelligence also provides specific leads of current foreign infiltrations of one's own side. As well as

evidence for counter-espionage, counter-intelligence can also provide intelligence on penetrations by other foreign intelligence sources, such as SIGINT. This can be used to improve the security defences concerned and prevent the opponent's exploitation of weaknesses.

Soviet security in the early Cold War was so effective partly due to defensive counter-measures built upon accurate inside information from spies inside the West. The damage caused by ideological spies like MI6 officer Kim Philby that lasted the longest was the exposure of Western technical sources in the early Cold War era. Soviet espionage continued to provide such coups against Western technical intelligence gathering. Intelligence on US satellite intelligence programmes collected in the 1970s offered the basis for the USSR's defensive security initiatives to reduce the effectiveness of US surveillance satellites. During the 1980s, the cases of British GCHQ linguist Geoffrey Prime and the American Ronald Pelton, both Soviet agents who provided Moscow with details of US-UK successes against Soviet communications, also revealed Soviet counter-intelligence infiltration. In this sense, intelligence opponents are locked in a counter-intelligence contest - trying to capture or penetrate each

Counter-intelligence work impacts on all security agencies - including the USS Secret Service



other while themselves avoid being captured or penetrated.

OPERATIONAL INFERENCES

Inferences about an adversary's intelligence successes can also be drawn from observation of the opponent's non-intelligence activities which intelligence supports.

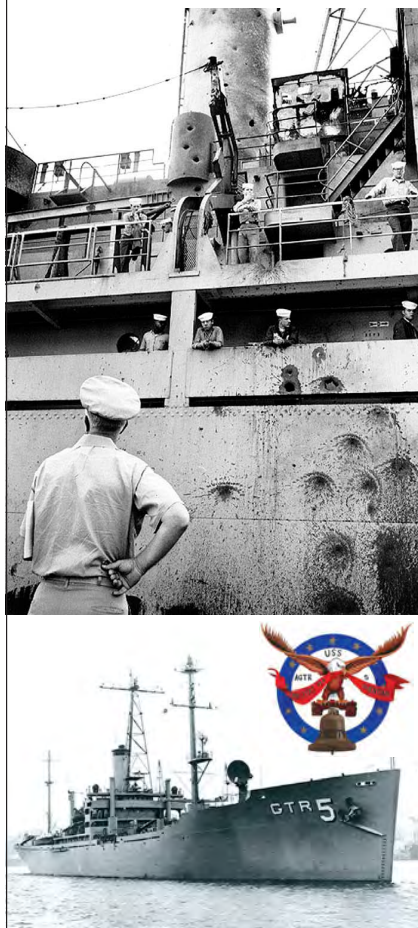
Total support for information security involves checking incoming intelligence about enemy



The interception of German WWII signals was crucial in helping to counter the activities of U-boats. Unfortunately Enigma (machine pictured) couldn't prevent the sinking of the Dixie Arrow, an Allied tanker torpedoed by U-71 in the North Atlantic, 1942

forces and their communications for indications that their actions reflect intelligence-derived knowledge of one's own side. An important part of British SIGINT analysis during the Second World War was checking

The US Navy spyship USS Liberty was attacked by Israel in waters off the Sinai Peninsula in 1967. The controversial incident claimed the lives of 34 US personnel



decrypted German messages for indications that Germany had broken any Allied ciphers or codes. However, this kind of analysis of foreign intelligence collection requires a dedicated effort specifically assigned for the task. Although they gathered mounting evidence of the superiority of Allied intelligence during the Second World War, the Germans steadfastly refused to believe that Enigma could be deciphered. Britain was similarly complacent regarding its own vulnerable naval ciphers during the early stages of the Second World War. Revelations that the KGB had broken US naval ciphers in the 1970s and 1980s, due to material provided by the Walker family spy-ring, seem to have caught the USA totally by surprise.

ADVICE AND STANDARDS

Intelligence also acts as part of the security system itself - using its offensive expertise in the defensive role of poacher turned gatekeeper.

Intelligence supplies specialised security material and sets defensive standards. On top of its intelligence concern for internal threats, MI5 is also responsible for defensive security standards against HUMINT attacks, including the vetting of people and safeguarding documents. These duties are so broad in scope that MI5 is a defensive security organisation as well as an intelligence organisation. Similarly, cipher-breakers are viewed as the best cipher-makers. As early as the eighteenth century, British cipher-breakers were asked to devise their own states' ciphers. More recently, it has become best practice for SIGINT organisations to be responsible for Comsec and Compusec (communications and computer security). Eavesdropping experts provide technical advice to those developing devices to counter



Counter-intelligence king. The FBI's longest serving Director trusted few people or organisations, including some from 'friendly' nations

eavesdropping. Those devising camouflage schemes should seek advice from photo-interpreters. Thus, the quality of offensive intelligence experience helps to determine the quality of the defence. In some cases, technical research and development can be supported for both offensive and defensive purposes.

SECURITY RESPONSIBILITIES AND INTELLIGENCE CONTESTS

Intelligence's relationship with security is closer than normal intelligence customers.

The operational arms of government have responsibility for security, but intelligence makes the inputs just set out above. One effect of this is to place important executive and advisory responsibilities within their national information security systems on parts of the intelligence community. A second effect of information security needs is the commitment of part of intelligence to the counter-intelligence battle with its adversary's. All intelligence gathering is part of a contest against opposing security systems. However, the counter-intelligence contest should be viewed as separate from this main intelligence-security battle. The counter-intelligence contest is intelligence's specialised attempt to infiltrate foreign intelligence, while attempting to inhibit it from attacking one's own side.

EYE SPY

INTELLIGENCE MAGAZINE

SUBSCRIBE

A subscription will protect you
against any price increase

UK, USA, CANADA, EUROPE, ROW

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

UK 1 YEAR £29.95 ☐ USA 1 YEAR \$49.99 ☐ EUROPE/ROW 1 YEAR £32.00 ☐

UK 2 YEAR £55.00 ☐ USA 2 YEAR \$96.00 ☐ EUROPE/ROW 2 YEAR £60.00 ☐

Name: _____ Address: _____

Post/Zip Code: _____ Country: _____

email: _____

Cheques must be payable to: **'EYE SPY PUBLISHING LTD'**

NOTE: WE ONLY ACCEPT UK, USA AND CANADIAN CHEQUES

I enclose Cheque for: _____ / _____



For credit card payment by Visa, MasterCard, American Express

Credit Card No: _____

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

reverse of the credit card: _____

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



UNITED STATES OF AMERICA

Mail your subscription to:

Eye Spy International
Empire State Building,
350 Fifth Ave,
59th Floor, New York,
NY 10118-0069



UK, EUROPE, ROW

Send your subscription to:

Eye Spy Publishing Ltd
P O Box 10,
Skipton,
Leeds City Region,
BD23 5US,
United Kingdom



CANADA

Send your subscription to:

Eye Spy
Intelligence Magazine,
Canadian Bureau,
Unit 102,
2054 Courtland Drive,
Burlington, Ontario,
L7R 1R8

By Telephone 01756 770199
12.00pm - 6.00pm, Mon-Fri

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



ESPL_2017_ESTONIA_GATES108/108/108



Counter-intelligence should be seen as a set of sub-contests subordinate to the main intelligence-security contest. The first level is counter-intelligence: counter-intelligence's targeting of the adversary's intelligence. For example, possessing an agent within the opponent's intelligence community discloses the identity of his agents, so that they can be eliminated. Inside this first level contest is a second level, counter-counter-intelligence: penetration targeted against the adversary's own counter-intelligence effort, in order to learn if he has infiltrated one's offensive intelligence campaign. Success offers the prospect of not only neutralising the intelligence threat but of capturing it - gaining a position in which the adversary's intelligence community is under one's own control without the opponent's knowledge.

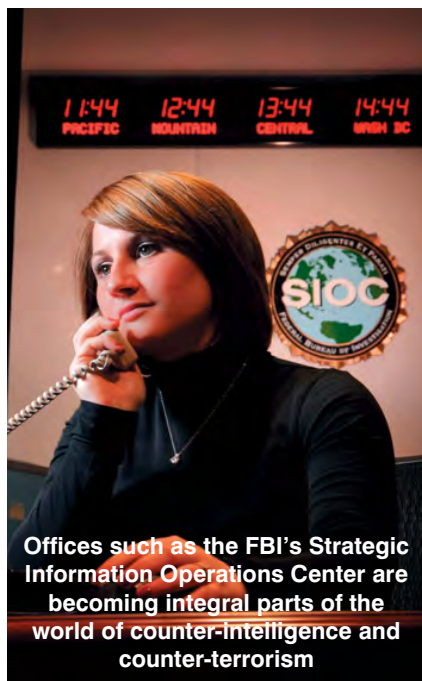
DECEPTION AND CONTROL

Counter-intelligence is never as total as this might suggest, but examples can be shown of counter-intelligence's successes. For example, at the first level, the British agent network directed from the Netherlands was completely rounded-up by the Germans at the start of the Second World War due to British underestimation of the risk of infiltration. During the Cold War, Philby gave the KGB details of Western agents; and Western spies like Oleg Gordievsky did the same in reverse. Some Western intelligence networks in the Soviet Union were discovered in their early stages and then operated under the USSR's control. An example of how agents inside intelligence can cause close-range intelligence gathering to be neutralised is when MI6 officer George Blake provided his Soviet handlers with details of US-UK tapping of the USSR's cables in



Berlin (See Eye Spy 107). Access to the adversary's intelligence community at this level also offers the chance of detailed control over deception. The successful British deception regarding the timing and location of the Normandy landings during the Second World War, by capturing and turning Abwehr agents and deciphering Abwehr messages, are perfect examples of having a part of the adversary's intelligence system under one's own control and being in position to fine-tune the deception operation.

The Cold War also witnessed infiltrations at the second level of the counter-intelligence contest: gaining access to the adversary's



Offices such as the FBI's Strategic Information Operations Center are becoming integral parts of the world of counter-intelligence and counter-terrorism

DRUGGED AND QUESTIONED

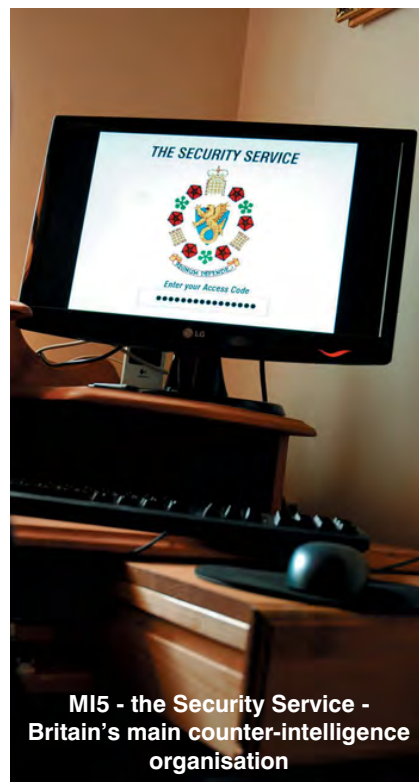


MI6 pulled off an intelligence coup for the West as KGB man Oleg Gordievsky defected to the UK in 1985. He is seen in this White House photograph from 1987 sitting next to President Ronald Reagan. Interestingly, just before his dramatic escape, he was drugged by KGB counter-intelligence officers and questioned. Moscow had been tipped-off he was a spy - but failed to prove the allegation... the rest is history.

own counter-intelligence service. Philby was the head of MI6 counter-intelligence. As a Soviet agent in that role, he not only warned his Soviet controllers that one of their intelligence officers based in Turkey had requested British asylum, Philby was also able to delay the British response to this asylum request until the KGB had been able to neutralise the potential defector. Almost a mirror-image of this occurred in 1983, when disillusioned MI5 officer Michael Bettaney offered his services to the Soviets, but Oleg Gordievsky, an MI6 agent inside the KGB's London residency, warned the British intelligence services, who had Bettaney apprehended. Gordievsky was himself subsequently betrayed to the KGB by Aldrich Ames, a member of the CIA's counter-intelligence branch spying for the Soviets.

In addition to these counter-intelligence coups, agents recruited from within foreign intelligence services can also provide invaluable non-intelligence information. For example, Penkovsky and Gordievsky provided information on a wide range of Soviet political and military activities, not just the activities of Soviet Intelligence.

Thus, counter-intelligence has many ramifications. Counter-intelligence's primary role is to safeguard information security by penetrating foreign intelligence services that pose a threat to it. Counter-intelligence's secondary purpose is to defend its own intelligence attacks by infiltrating the adversary's counter-intelligence. Success in these counter-intelligence contests can pay huge dividends, which explains Intelligence's seemingly incestuous focus on its opposite numbers throughout the Cold War. However, even during the Cold War, when the threat from Soviet Intelligence loomed so large, Western Intelligence's role in supporting information security required only a small part of intelligence's resources. Providing defensive information security advice does not require that much manpower or expense. Counter-espionage was a large, but not unbearably costly, part of security intelligence.



MI5 - the Security Service - Britain's main counter-intelligence organisation

Counter-intelligence is a specialised function that looms larger in spy novels than in normal day-to-day intelligence work!

CONCLUSION

As this series has shown, every kind of offensive intelligence gathering breeds a related defensive technique. Counter-intelligence is relatively cheap. It certainly costs only a fraction of the damage that can be done by a hostile intelligence service that succeeds in breaching one's security defences. Whole agent networks can be compromised by double-agents like Philby. Hugely expensive IMINT and SIGINT programmes can be negated for only a few thousand dollars, by buying technical manuals and codebooks from greedy and/or disgruntled current or former intelligence personnel like Kampiles and Walker. The need for counter-intelligence did not come to an end with the ending of the Cold War.

A WARNING

Regular readers of Eye Spy will be familiar with the recent resurgence of Russian and Chinese espionage against the UK and USA. With the current focus on international terrorism, it seems that counter-intelligence is being somewhat neglected. In recent years, the UK's parliamentary Intelligence and Security Committee (ISC) has expressed concern that MI5's counter-espionage capability has suffered as resources have been moved into counter-terrorism.

© DR CHRIS NORTHCOTT 2017

PART 7

THE ART OF DISTRACTION

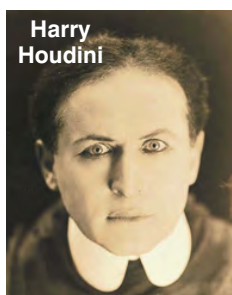
The Deceptive Factor

IN THE INTELLIGENCE CYCLE

Security specialist MIKE FINN examines various subjects associated with the art of distraction and how some aspects of this craft have been utilised by the intelligence world

Have you ever felt your thoughts were not your own; did you ever have an uneasy feeling your decisions felt manipulated? Even in the First

World War, research began into methods of manoeuvring peoples' thoughts and ideas. In Britain for example, the War Propaganda



Harry Houdini

Bureau was set up at Wellington house around 1914 - the objective being to develop effective ways of influencing thoughts and decisions.

With this in mind it is no wonder that

British Intelligence used Harry Houdini; later, the CIA recruited the conjurer Mulholland, and so it went on. The focus was clearly on finding methods to influence the mind and the decisions it produced.

One way of categorising the skills that the intelligence world gained from the knowledge of conjurers was to look at the use of the primary ingredients, which are confusion and manipulation; these were covered in previous articles. The third factor is the art of distraction, which we will now examine. Distraction is a ploy to divert attention, or break concentration.

The principles of distraction have multi-faceted use, so we will first look at a generalisation of how diverse this field is. In principle the mind can only focus on one intense task at a time.



Fagin - a Charles Dickens character skilled in the art of deception and pick-pocketing

By way of example, you can drive a car and have a conversation, it can not be a meaningful one or driving perception will reach a danger risk level. If you want to draw someone's attention away from one task to another, in order to facilitate your access to the first task, then distraction is the best method to use.

The more the art of distraction is understood, the more efficiently this task can be accomplished. It may be a phone call to get someone out of an office, or a request for something from a filing cabinet, in order to remove a document from a table while a person's back is turned. The ingenuity of distraction is the gateway to success.

DEAD DROPS AND DISTRACTION

In espionage, the information chain of the agent or spy is controlled by a handler; this operative oversees the various assignments. The handler usually arranges how information will be retrieved and exchanged, but it's the courier who collects and delivers information, which can be performed in two ways. A 'live drop' is when a courier exchanges items or information directly, while a 'dead drop' is where information is left and collected from a secret location. In both cases distraction plays a prominent role, creating a way of drawing attention from the exchange, often at the moment it takes place.

The need for understanding the art of deception has a paramount role in all areas of intelligence. James Angleton, head of counter-intelligence (CIA from 1954 - 1974) coined the phrase 'wilderness of mirrors' to encapsulate deception in terms of strategies and smoking



Any distraction whilst driving lessens control of a vehicle

mirrors, which in particular, the Soviet Union employed in an attempt to confuse and split the Western world as part of its Cold War strategy. I am sure by now you can perhaps see many areas where the art of deception has a role in the intelligence cycle. However, it still does not portray the root principles of deception. Whilst the CIA gleaned such principles from people like Mulholland, I think a better direction of understanding is to examine the art of the pickpocket.

Much of the pickpocket's success relies on diverting attention and breaking concentration as they implement their craft. A classic example is the basic setup, where one person acts as the 'distracter', drawing the attention of the 'mark' - the target figure. The pickpocket performs the actual task and is known as the 'dip'. Since the time of Charles Dickens' famous Fagin, pick pocketing has been a well known criminal art. Without distraction skills it would not be possible, the same of course applies to the intelligence world.

I remember when I was in my late teens, attending an evening session at an art school. One of the students was also a stage pick-pocket (magician). He would wander around, stand behind you as you were drawing, then hold your wrist in an appreciative way and say things like "that's great, much better than I could do." At the end of the class he stood by the door and gave everyone their watch back - however, even though the students knew what had happened, he was able to repeat it the following week.

It's amazing that so many people seem 'happy' to be vulnerable. When I was part of an anti-pick-pocket squad, we warned the public over and over. Nevertheless, almost no one took any notice of our advice, even though it could have protected them. Wallets still stuck out from back pockets, purses were put back on top of bags; to the pick-pocket it was as easy as taking



Pick-pocket distraction

candy from a baby. However, this is just a comparison to help you understand how far reaching one well applied principle can be.

In this article I have drawn the analogy with 'dips' because it is a visual example that epitomises the skilful use of distraction. Once you can clearly see the structure of principle, then it is easier to see how such methods are used in the intelligence cycle.

Since the time that Houdini, Mulholland and others began the expanding spiral of this unusual knowledge, the door has been opened to some fascinating aspects of mind manipulation within the intelligence cycle. I will deal with this in the next issue and touch on the subject of 'psy-ops'.



Artist Hieronymus Bosch's painting 'The Conjurer' CIRCA. 1500. A pick-pocket joins with a conjurer who distracts one interested onlooker as he removes his purse



A German police officer in Hannover with a mannequin warning of thieves and pick-pockets



ANOTHER DARK DAY IN LONDON

details in order that MI5 could identify associates and help plan the raids.

A detailed 1,000-page study released in February, revealed Birmingham as one of the 'terror recruitment capitals of the world'. Between 1998 and 2015, 49 of 269 people convicted of Islamist terrorism offences or killed performing suicide attacks were from the West Midlands.

ARRESTS

Following the Westminster attack, 11 people were detained, friends, associates and a family member. Those arrested include a 39-year-old woman held at an address in east London on suspicion of the preparation of terrorist acts. An indication, perhaps, she was aware he intended to carry out the attack. Computers and cell phones were recovered, but despite investigators calling two arrests "significant," all but one had been released less than 72-hours after Masood's rampage. Evidence again that he had acted alone.

24 HOURS LATER

The police investigation, codenamed Operation Classific, saw eight addresses raided by CT



Acting Deputy Commissioner
Mark Rowley



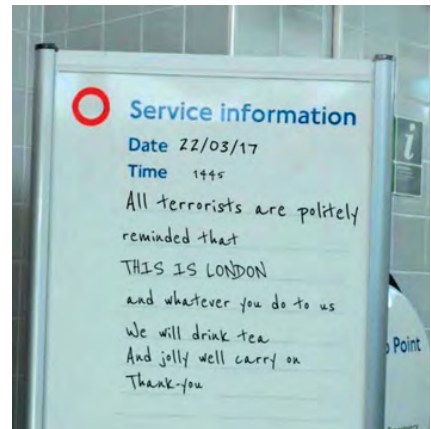
Armed police in Whitehall - note the pavement counter-vehicle attack pillars

forces, and searches of 16 properties. Over 2,700 items have been seized. Police made contact with 3,500 people in relation to the incident, including 1,000 in the Westminster Bridge area and 2,500 who were on the Parliamentary estate during the attack. Cell phone photographs and footage was secured and eye-witness testimony acquired.

Acting Deputy Commissioner, Mark Rowley, said: "Our investigation focuses on [Masood's] motivation, his preparation and his associates. While there's still no evidence of further threats, you will understand our determination is to ascertain whether he acted totally alone or was inspired by terrorist propaganda or if others have encouraged supported or directed him," said Rowley, who is also head of the organisation's Counter Terrorism Command (CTC).

A LONE WOLF TERRORIST?

The terrorist, born Adrian Elms, in Dartford Kent 1964, became Adrian Russell Ajao following his mother's marriage. It was one of at least five identities he used in various locations across the UK, Saudi Arabia and his time spent in the prison system. He had various previous convictions including assault, GBH (grievous bodily harm), possession of offensive weapons and public order offences. It is believed he converted to Islam while in jail

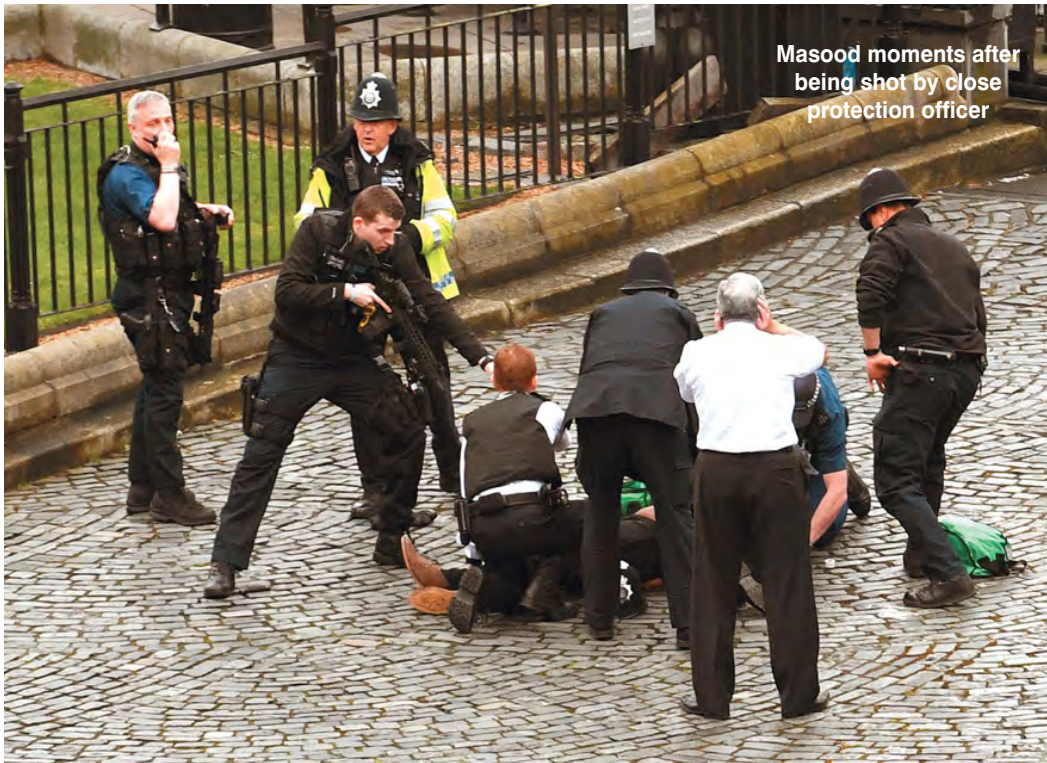


and sources believe he may have become more hardline after working in Saudi Arabia as an English teacher.

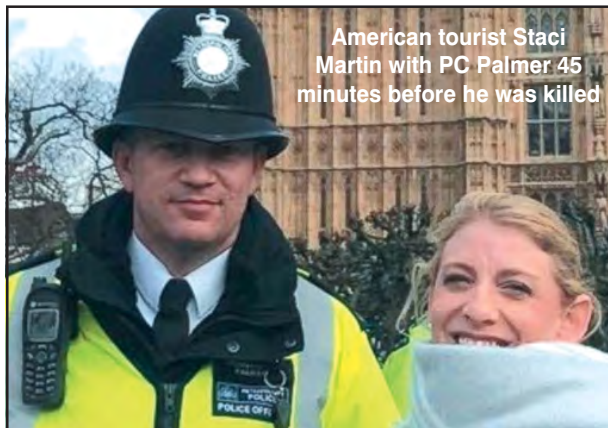
Masood was investigated by MI5 for alleged links to Al-Muhajiroun (ALM). The Security Service was alerted to Masood in the aftermath of the 2005 London terror attacks because he attended meetings hosted by Anjem Choudary. Choudary, was sentenced to



Entrance to Masood's
flat in Birmingham



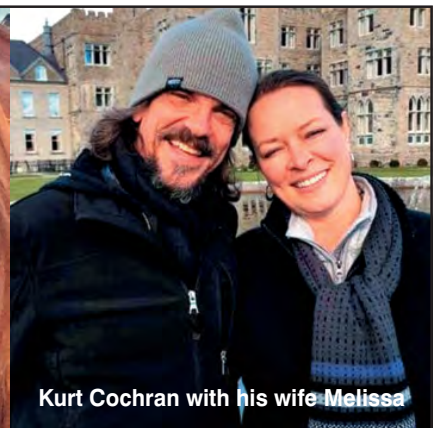
Masood moments after being shot by close protection officer



American tourist Staci Martin with PC Palmer 45 minutes before he was killed



Aysha Frade



Kurt Cochran with his wife Melissa

© SHANTELL PAYNE

five years in prison in 2016 for supporting ISIS and urging people to join the terror group.

THE CASUALTIES

In addition to NSY officer Palmer, Aysha Frade, 43, a married Spanish teacher with two daughters died. She was killed on Westminster Bridge on her way to pick up her children from school. Also killed on the bridge was American tourist Kurt Cochran, in London celebrating his 25th wedding anniversary with his wife Melissa; Leslie Rhodes, 75, a retired window cleaner from Streatham, south London, who once tended the windows of Winston Churchill's home Chartwell. He had his life support withdrawn at King's College



© NSY/BROWN COPYRIGHT

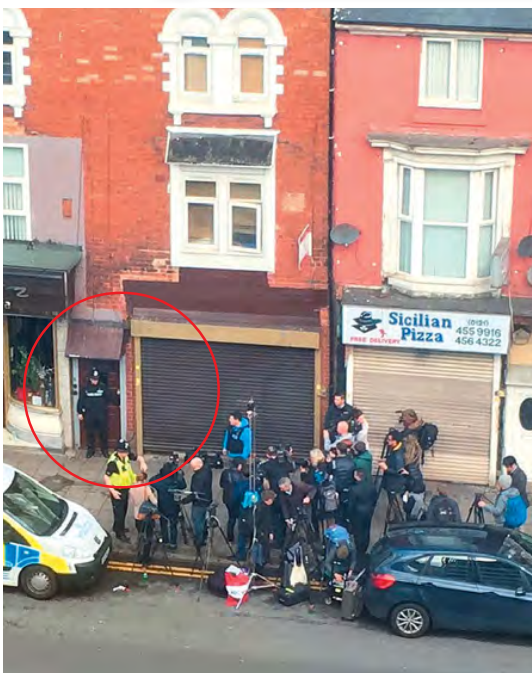
Leslie Rhodes

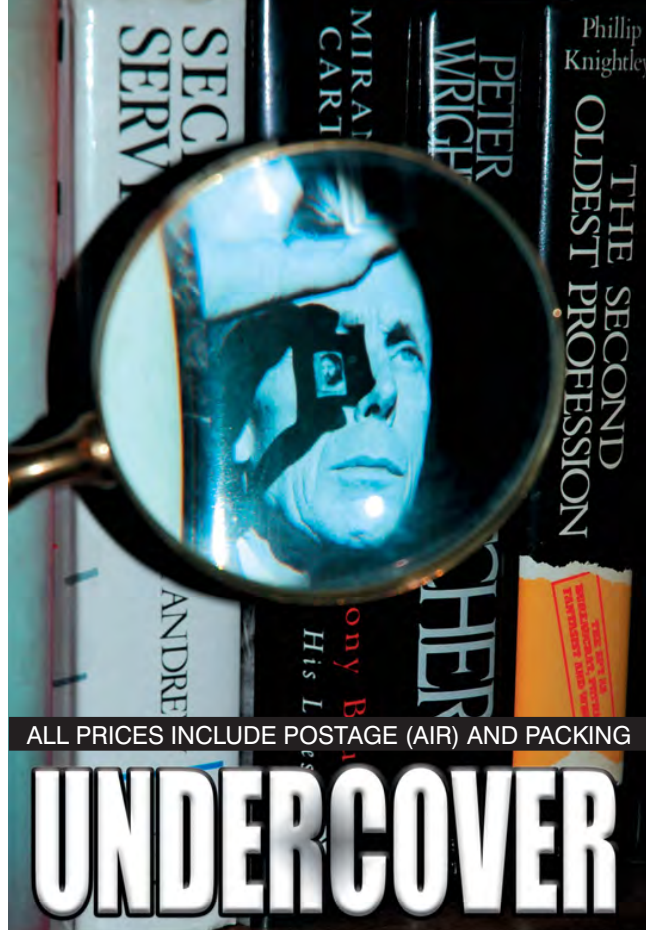


Hospital and died. Of the estimated fifty injured, seven remain in critical condition - including two police officers.

On 27 March, a 30-year-old man was arrested in Birmingham on suspicion of preparing terrorist acts - this in connection with the London attack. Police removed several bags of items from his residence, including computers and CDs. The only other person still held is also from the city.

Senior detectives already acknowledge at this early stage, "we may never fully understand the reasons why Masood did this."





ALL PRICES INCLUDE POSTAGE (AIR) AND PACKING

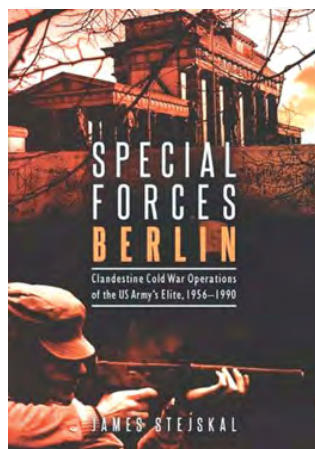
UNDERCOVER

BOOK RELEASES

SPECIAL FORCES BERLIN:
Clandestine Cold War Operations
of the US Army's Elite 1956-1990
 James Stejskal
 Casement

It is a little-known fact that during the Cold War, two US Army Special Forces detachments were stationed far behind the Iron Curtain in West Berlin. The existence and missions of the two detachments were highly classified secrets.

The massive armies of the Soviet Union and its Warsaw Pact allies posed a huge threat to the nations of Western Europe. US military planners decided they needed a plan



to slow the juggernaut they expected when and if a war began. The plan was Special Forces Berlin. The first 40 men who came to Berlin in mid-1956 were soon reinforced by 60 more and these 100 soldiers (and their successors) would stand ready to go to war at only two hours' notice, in a hostile area occupied by nearly one million Warsaw Pact forces, until 1990.

Their mission should hostilities commence was to wreak havoc behind enemy lines, and buy time for vastly outnumbered NATO forces to conduct a breakout from the city. Softback 336pp

Available from Eye Spy Ref: ES/1665
 UK £27.50 USA \$38.00 ROW £28.50

A SECRET WELL KEPT: The
Untold Story of Sir Vernon Kell

Constance Kell
 Conway

Britain's domestic counter-intelligence and security agency, more commonly known as MI5, was founded in 1909 by Sir Vernon Kell KBE. Kell not only founded MI5 but was also its Director for 31-years, the longest tenure of any head of a British government department during the twentieth century. Kell was also



Vernon Kell

fluent in six foreign languages, making him arguably the most gifted linguist ever to head a Western intelligence agency.

A Secret Well Kept was written by Kell's wife, Constance, in the 1950s, and the manuscript has been a treasured family possession ever since. Constance's story is endlessly fascinating: she tells of their life in China during the Boxer Rebellion, the formation of MI5 in 1909, the key characters, events and spy cases of Kell's career, and his important work achieved for the country during two world wars.

A modern-day preface from Kell's great-granddaughter, introduction by Stewart Binns and notes from Eye Spy associate editor Dr Chris Northcott add historical context to this delightful and unparalleled insight into the personal life of an extremely powerful and important man. Hardback 224pp

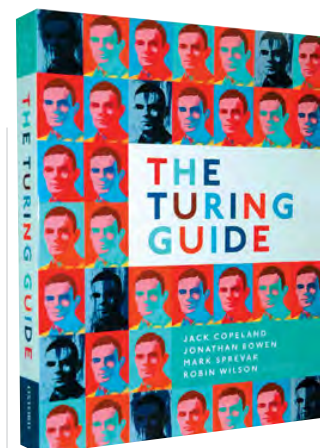


Available from Eye Spy Ref: ES/1666
 UK £20.00 USA \$35.00 ROW £21.00

THE TURING GUIDE

Jack Copeland, Jonathan Bowen,
 Mark Sprevak, Robin Wilson
 Oxford University Press

Alan Turing has long proved a subject of fascination, but following the centenary of his birth in 2012, the code-breaker,



computer pioneer, mathematician (and much more) has become even more celebrated with much media coverage, and several meetings, conferences and books raising public awareness of Turing's life and work.

This superb and huge volume brings together contributions from some of the leading experts on Alan Turing to create a comprehensive guide to Turing that will serve as a useful resource for researchers in the area as well as the increasingly interested general reader.

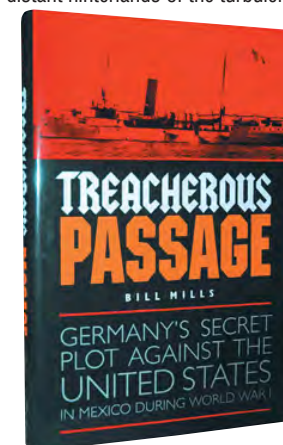
The book covers aspects of Turing's life and the wide range of his intellectual activities, including mathematics, code-breaking, computer science, logic, artificial intelligence and mathematical biology, as well as his subsequent influence. Large Softback 576pp

Available from Eye Spy Ref: ES/1667
 UK £23.99 USA \$42.00 ROW £25.99

TREACHEROUS PASSAGE:
Germany's Secret Plot Against
the United States in Mexico WWI

Bill Mills
 Potomac Books Inc

While the Great War raged across the trench-lined battlefields of Europe, a hidden conflict took place in the distant hinterlands of the turbulent



Mexican Republic. German officials and secret service operatives plotted to bring war to the United States through an array of schemes and strategies, from training a German-Mexican army for a cross-border invasion to dispatching saboteurs to disrupt American industry and planning for submarine bases on the western coast of Mexico.

Bill Mills tells the true story of the most audacious of these operations: the German plot to launch clandestine sea raiders from the Mexican port of Mazatlán to disrupt Allied merchant shipping in the Pacific.

The scheme led to a desperate struggle between German and American secret agents in Mexico. Full of drama and intrigue. Hardback 280pp

Available from Eye Spy Ref: ES/1668
UK £27.00 USA \$38.00 ROW £28.00

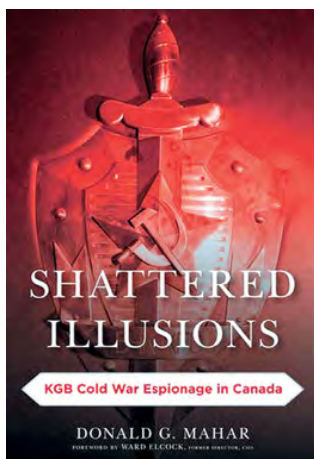
SHATTERED ILLUSIONS: KGB Cold War Espionage in Canada

Donald G. Mahar, Ward Elcock
Rowman & Littlefield Publishers

Yevgeni Vladimirovich Brik and James Douglas Finley Morrison were central figures in what was considered one of the most important Cold War operations in the West at the time.

Yevgeni Brik was a KGB deep cover illegal who had been dispatched to Canada in 1951. He settled in Verdun, Quebec. He eventually became the KGB Illegal Resident where he had responsibility for running a number of agents, one of whom was working on the CF-105, Avro Arrow. In 1953, he fell in love with a married Canadian woman to whom he revealed his true identity. She persuaded him to turn himself in, which resulted in his becoming a double agent, working for Canada. He was later betrayed by a Royal Canadian Mounted Police Officer, James Morrison, who sought money from the KGB to pay his debts.

Brik was consequently lured back to Moscow in 1955, where he was arrested, and interrogated. Convicted of treason, a traitor's fate awaited him, predictable, grim and final. Incredibly, he reappeared at a British Embassy as an old man in 1992, seeking Canada's help. He was exfiltrated by a joint Canadian/



British intelligence team headed by Donald Mahar. Softback 262pp

Available from Eye Spy Ref: ES/1669
UK £31.50 USA \$38.00 ROW £28.50

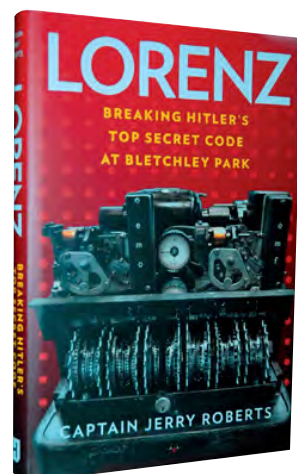
LORENZ: Breaking Hitler's Top Secret Code at Bletchley Park

Jerry Roberts
The History Press

The breaking of the Enigma machine is one of the most heroic stories of the Second World War and highlights the crucial work of the codebreakers of Bletchley Park, which helped prevent Britain's defeat in 1941. But there was another German cipher machine, used by Hitler himself to convey messages to his top generals in the field. A machine more complex and secure than Enigma. A machine that could never be broken.

For sixty years, no one knew about Lorenz or 'Tunny', or the determined group of men who finally broke the code and thus changed the course of the war. Many of them went to their deaths without anyone knowing of their achievements.

Here, for the first time, senior codebreaker Captain Jerry Roberts



Lorenz cipher machine

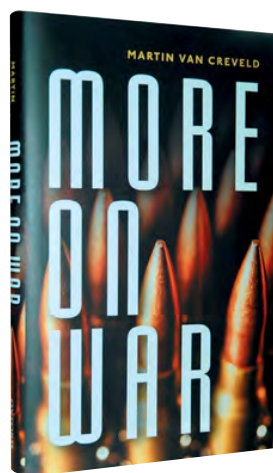
tells the complete story of this extraordinary feat of intellect and of his struggle to get his wartime colleagues the recognition they deserve. Hardback 240pp

Available from Eye Spy Ref: ES/1670
UK £22.99 USA \$35.00 ROW £24.99

MORE ON WAR

Martin van Creveld
Oxford University Press

According to Martin van Creveld, one of the world's best-known experts on military history and strategy, "War is the most important thing in the world." The survival of every country, government, and individual is ultimately dependent on war - or the ability to wage it in self-defence. That is why, though it may come but once in a hundred years, it must be prepared for every day.



Nevertheless, in spite of the centrality of war to human history and culture, there has for long been no modern attempt to provide a replacement for the classics on war and strategy, Sun Tzu's *The Art of War*, dating from the 5th or 6th century BC, and Carl von Clausewitz's *On War*, written in the aftermath of the Napoleonic Wars.

What is needed is a modern, comprehensive, easy-to-read and

understand theory of war for the 21st century that could serve as a replacement for these classic texts. The purpose of this book is to provide just such a theory. Hardback 240pp

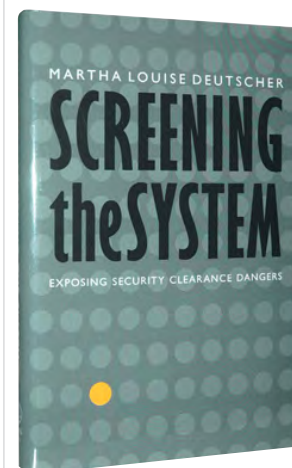
Available from Eye Spy Ref: ES/1671
UK £22.00 USA \$32.00 ROW £23.00

SCREENING THE SYSTEM:

Exposing Security Clearance Dangers

Martha Louise Deutscher
Potomac Books Inc

Martha Deutscher believes the Personnel Security Clearance System - the process by which the US federal government incorporates individuals into secret national security work - is flawed. The author explores the current system and the amount of power afforded to the state in contrast to that afforded to those who serve it.



It is a timely examination of the US screening system and shows how security clearance practices, including everything from background checks and fingerprinting to urinalysis and the polygraph, shape and transform those individuals who are subject to them.

By bringing participants' testimonies to light, Deutscher looks at the various practices while revealing cultural insights into the way we think about privacy, national security, patriotism and the state. *Screening the System* provides recommendations for a more effective method that will be of interest to military and government professionals as well as policymakers and planners who work in support of US national security. Hardback 216pp

Available from Eye Spy Ref: ES/1672
UK £24.00 USA \$34.00 ROW £24.00



UNINTENTIONAL ENTRAPMENT

One person who falls into this category is former US Army Lt. General Michael Flynn - President Trump's National Security Advisor. He had occupied the position for just 24 days before information surfaced which forced the highly experienced intelligence man to resign. And it all stemmed from a simple telephone call made to Sergey Kislyak - the Russian Ambassador to the United States in 2016.

Flynn reportedly discussed President Obama's range of sanctions imposed on Moscow following the hacking of Democratic computers and e-mails. This hacking in itself was a form of subtle entrapment leading to all manner of internal squabbles and debate amongst the politicians involved. News of the telephone call leaked, but Flynn initially denied discussing the affair with Kislyak. Even Vice President Pence denied Flynn had communicated with the Russians. However, there was no let up in the criticism, and his 2015 contacts with RT (regarded as a Russian propaganda front by some intelligence watchers) came back to haunt him. Eventually Flynn stepped down after calling himself a "lightning rod." It was an apt description. But the American media went further saying the liaison made him vulnerable to entrapment.



INTEL INSIDE

Above: Former Trump National Security Advisor Michael Flynn pictured next to President Putin at the Russia Today (RT) gala dinner. Despite this being a quite legitimate event and planned encounter, images such as this have been used by some in the media to 'illuminate' his alleged relations with Russia.

Another senior Trump man now caught up in the Russian business is US Attorney General Jeff Sessions. Like Flynn, there were stories that he had contact with Russian Ambassador to the USA Sergey Kislyak whilst serving on the US Senate Armed Services Committee last year. Sessions reportedly denied "any knowledge of contact" in January 2017. Some journalists contend Kislyak is a senior intelligence officer - others have labelled him a "Moscow spy." Russia's Foreign Ministry described the spy allegation as "the low professional standards of the American news media." Sessions has since removed himself from the FBI investigation into suspected Russian interference in the 2016 US General Election.

Which ever way one views these episodes, it identifies perfectly how past innocent actions and conversations can implode and be exploited by opponents.



In his defence, Flynn, said because of the “fast pace of events he inadvertently provided incomplete information.” All of this is now irrelevant, but undoubtedly his public election campaign support of Mr Trump against Hillary Clinton was also a factor.

ESPIONAGE AND THE PRIVATE SECTOR

One area of espionage difficult for any intelligence organisation to control is the private sector. And, to provide just one staggering fact regarding espionage in the corporate and business world, the FBI stated \$300 billion (£250b) of US intellectual property and business intelligence is stolen every year by a network of global players - including China, Iran, Russia and North Korea to name but a few. Some analysts believe this figure is incorrect and should be much higher, citing evidence that companies are reluctant to share all losses in the event it impacts on confidence.

Though the exact way in which losses are ascertained can't be fully understood, save cyber attacks and the 'capture' of technology and impact on business deals, much material disappears physically, through the unintentional and sometimes blase security methods deployed by travelling business people, scientists and government representatives. A large percentage will be included in the section corporate espionage, of which some will have direct threads to entrapment.



FBI analysts. The Bureau is but one of several US Government agencies investigating Russia's alleged interference and cyber operations targeting American individuals and organisations involved in the race for the White House. The CIA, NSA, ODNI, Justice Department and the Treasury Department's Financial Crimes Enforcement Network are all represented.

**INTEL
INSIDE**

Just like the warnings issued to British G20 delegates, overseas players are issued with warnings and briefed on personal safety and activities. However, many carry incredibly detailed dossiers containing materials which are of immense value to rival companies, rogue nations and those simply intent on theft and then re-selling to the highest bidder. It's an underworld activity that constantly haunts services such as MI6 and the CIA. And to

qualify and ascertain that such operations are real, it is not unusual for the CIA and others to establish front companies to test penetration in some countries. [In the 'language of spies' this is known as a form of positive entrapment]. Whilst such activities allow for the enabling of some counter-measures, especially in the area of advice to international businesses, it is hardly secure. ➤



Russian Ambassador to the USA Sergey Kislyak (centre) with President Vladimir Putin. Some journalists allege Kislyak is an intelligence officer and spy - a claim 'rubbished' by Moscow



arrived at his destination - thus it is intelligence protocol never to pack such items in checked baggage.

Beyond the conference room and meeting table, and often in casual and less traumatic environments, conversations take place where information is imparted. Some hotels and rooms, as identified, are specially adapted to secure all manner of information, and hotel WiFi is easily penetrated and monitored. Henceforth, it is best never to use such facilities. However, in certain situations where it is essential to make contact, some services can be sourced which encrypt messages.

Former MI6 officer Christopher Steele's 'Trump Dossier' is not unique. Such items are produced regularly and for various reasons, including entrapment and compromise.

For the best part of 20 years, the KGB targeted the Royal Family and members of the House of Windsor's entourage. Many of the operations were directed by Colonel Vadim Goncharov, chief scientific and technical

officer of the 5th Special Department. Princess Margaret in particular, was given special focus, especially her private life. Goncharov was instructed to compile a dossier on Margaret which contained alleged details of her brief 1967 love affair with Robin-Douglas Home, a society figure in the 1950s and 1960s. He committed suicide in 1968 aged just 36. There are other names which feature in the KGB file, including Roddy Llewellyn and Colin Tennant. Numerous hotels were bugged and all manner of encounters and conversations logged. One suspected target was therapist Kay Kierman who treated both the Queen and Margaret.

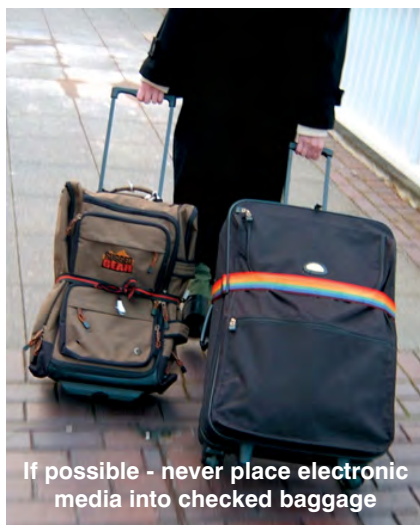
Following one operation, which took place whilst Margaret was visiting Denmark, Goncharov proclaimed he had secured information during the "bugging of drunken parties of the [held by] British Princess Margaret." Goncharov, however, later admitted that the Copenhagen operation did not reveal any lovers. "On this occasion our intention was in getting confidential information which would open certain doors for us," he said.

In the 1960s and early 1970s, British Prime Minister Harold Wilson was also given 'special attention' by the KGB - the objective being compromise and then recruitment. During one visit to Moscow, Mr Wilson stayed at the National Hotel next to the Kremlin. His room was bugged and all manner of attempts to secure information which could be used against the premier were actioned.

In the hotel bar, Goncharov placed female KGB officers posing as prostitutes. The objective was clear - a honey trap to capture Wilson in a compromising pose or situation with one of the girls. And whilst the KGB man said film

TARGET SELECTION

Identifying a company target is relatively easy, and often begins with the announcement of a meeting. Thereafter a simple search through a hacked airline passenger list or hotel booking will reveal the traveller, and it's not too difficult to generate further background on just who that person is or his/her position in a company. Called 'elicitation' in the intelligence world, if an operation to steal information at source is state-sponsored, then the target is even more vulnerable. Add to this, many business people and government contract workers carry electronic media, thus further opportunities to secure background material presents itself. Targeting such items as laptops can even occur before the traveller has





Harold Wilson - KGB target

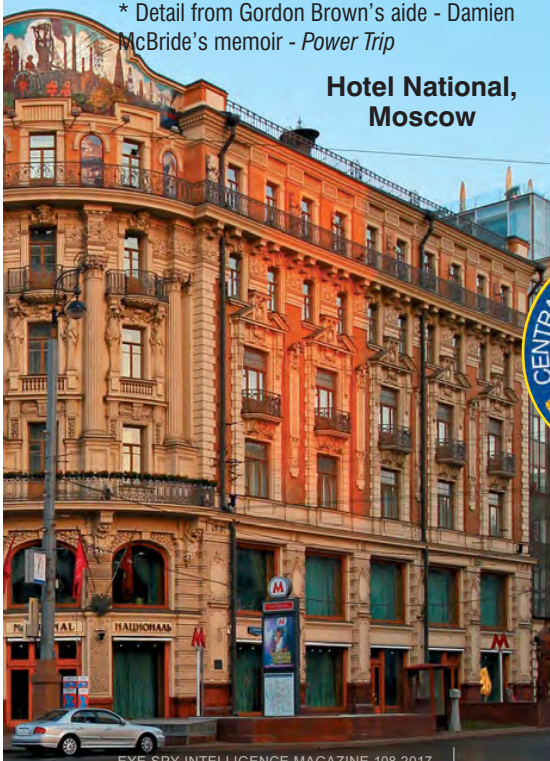
footage was taken, nothing of use was gleaned. He also believed Wilson, surrounded by staffers and intelligence people, was aware of the ruse.

These examples reflect the need for personal countermeasures to be taken seriously. A misdemeanour, behaviour, past association, act, liaison, meeting, conversation, affair, criminal activity, debt, divisive comment or even presenting a gift can be exploited by those intent on entrapment, threat and blackmail. These are just some areas that find favour with both those intent on espionage, intelligence recruitment, media mischief makers and the criminal community.

Entrapment occurs in all walks of life, but for key public figures and more importantly, for those who hold secrets and have keys to the secret world of intelligence and power, basic rules should be followed at all times - in all situations and environments. However, as Michael Flynn will testify, just a simple phone call can create a firestorm.

* Detail from Gordon Brown's aide - Damien McBride's memoir - *Power Trip*

Hotel National, Moscow



EYE SPY INTELLIGENCE MAGAZINE 108 2017

FANTASTIC VALUE!
FOR 2017
GIVE AN
EYE SPY
GIFT SUBSCRIPTION

NOW INCLUDES FREE ELECTRONIC SUBSCRIPTION

A GIFT SUBSCRIPTION NOW INCLUDES: FREE DIGITAL EDITION SUBSCRIPTION FOR ANY DEVICE OF YOUR CHOICE! PLUS EYE SPY'S US INTELLIGENCE SERVICES MOUSE MAT AND AN EYE SPY BINDER.... CALL FOR DETAILS OR VISIT www.eyespyimg.com (subscription section)

HIGH QUALITY EYE SPY BINDERS

Keep your Eye Spy magazines in pristine condition with these smart high-quality binders - each binder holds eight editions

PRICE INCLUDES P & P AIR MAIL

ORDER REF: ES/099 UK £7.50 USA \$17.00 EUROPE/ROW £10.00

US INTELLIGENCE SERVICES MOUSE MAT

Fantastic clarity - optical friendly

Eye Spy's brilliant US Intelligence Services mouse mat features the major agencies of America. Delivers superb mouse control - this full colour mouse mat will be a talking point in office and home!

ORDER REF: ES-MMUS UK £7.50 USA \$16.00 EUROPE/ROW £8.50

WATERGATE II

The 'Bugging' of Trump Tower

Continued from page 51

GCHQ SPY ALLEGATIONS

After much criticism and with no evidence to prove any US-based eavesdropping, the White House drew Britain's GCHQ into the affair. Claims it was behind the bugging were also rejected. Eventually, White House staffers tried to play down the 'wiretapping' comments and said the President was speaking in general terms. An exasperated NSA Director Michael Rogers said the eavesdropping claims against GCHQ were "untrue" and that the UK organisation was "frustrated" it had been accused in the first place.

Either way they were extraordinary claims, and come at a time when accusations continue to



Michael Rogers -
NSA Director



President Trump bids
farewell to President Obama

be made by senior figures over Trump's Russian liaisons. Many centre around Russia's Ambassador to the United States, Sergey Kislyak. Michael Flynn has already departed because of his conversations with Russian diplomats, but it has now transpired, at least six senior Democratic leaders have also met and talked to Kislyak - despite claiming otherwise.

As for Dan Rather, he stepped down in 2006 after the controversial reporting on CBS's 60 Minutes of President George W. Bush's National Guard service record. The broadcasting network questioned several aspects of Bush's service, all of which were eventually disproved.

*The word McCarthyism was first coined by cartoonist Herbert Block in the *Washington Post* 1950

LAST WORD

'HANDWRITING' OF MOSCOW NEW ASSASSINATION CASE

KIEV: As the world's attention focused on various terrorist attacks in major cities, another incident occurred in Ukraine which many intelligence watchers believe had all the hallmarks of a Kremlin-sanctioned action.

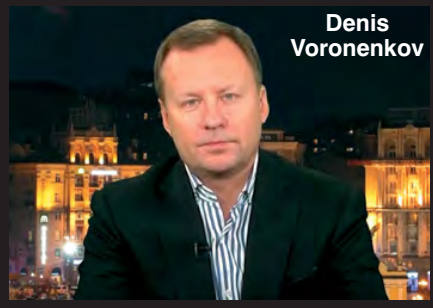
On 23 March, former Russian politician Denis Voronenkov was shot dead by an assassin near a hotel in Kiev. His bodyguard was injured in the attack.

Voronenkov had been granted sanctuary in Ukraine and had provided information on various alleged Russian actions in the country. He had become a "vociferous critic" of Putin. This, according to sources, made him a prime target.

Ukraine President Petro Poroshenko said the murder "clearly shows the handwriting of Russian special services... repeatedly shown in various European cities."

Kremlin spokesman Dmitry Pesko described the allegation of Russian involvement as "absurd."

Voronenkov renounced his Russian citizenship after claims he was being "persecuted by Russia's security services."



Denis
Voronenkov

OFFICIAL EYE SPY ORDER FORM 2017

Ref	Price	Ref	Price

Total £ or \$

Name _____

Address _____

Post/Zip Code _____ Country _____

Method of payment [A] Cheque [] [B] Credit card []

Cheques payable only to: **'EYE SPY PUBLISHING LTD'**

Card number _____

Expiry date _____

Last 3-digits on reverse of card (security code) _____



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, 59th Floor, New York,
NY 10118-0069, United States of America
Or Telephone TOLL FREE 877 309 9243



CANADA

Eye Spy Intelligence Magazine,
Canadian Bureau, Unit 102,
2054 Courtland Drive, Burlington, Ontario, L7R 1R8
Or Telephone TOLL FREE 877 309 9243

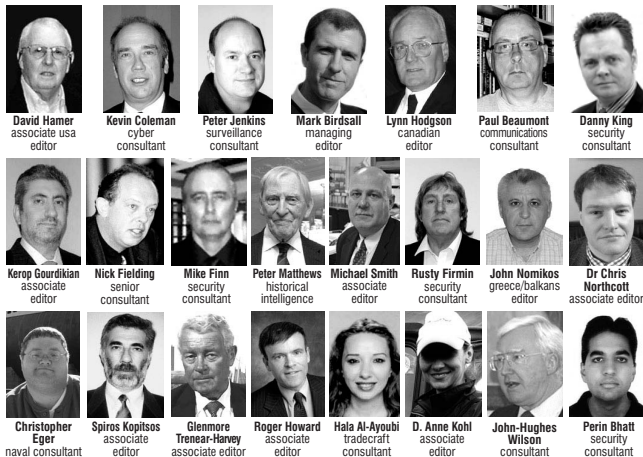
WE ACCEPT ORDERS VIA PAY PAL eyespy@eyespyimag.com

INTERNATIONAL INTELLIGENCE MAGAZINE

UK editorial address and head office: Eye Spy Publishing Ltd,
P. O. Box 10, Skipton, Leeds City Region, BD23 5US, England
Telephone: 01756 770199 UK
Office hours: 12.00pm - 6.00pm Monday to Friday GMT UK

USA editorial address and head office: Eye Spy Magazine International,
Empire State Building, 350 Fifth Ave, 59th Floor, 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
E-mail: support@eyespyimag.com • Web Site: www.eyespyimag.com

senior editors, consultants and feature writers



EYE SPY INTELLIGENCE MAGAZINE AVAILABLE ON NEWSSTANDS IN 60 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 (ESPL) or editor.

EYE SPY SUBSCRIPTION RATES WORLDWIDE

Annual subscription rates include air mail posting and packaging (eight editions)

united kingdom	£29.95
united states of america	\$49.95
europa	£32.00
canada	C\$60.00
australia/middle east/asia/africa	£32.00

please ensure cheques are payable to:
Eye Spy Publishing Ltd

Classified and 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.



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. It has no connection to any government organisation whatsoever. Points of view to the editor please



NORTH AMERICAN DISTRIBUTION

UNITED STATES OF AMERICA & CANADA -
Marketforce/Imagine +44 020 3148 UK



UK • EUROPE • ROW DISTRIBUTION

UK, Europe, Australasia, Rest of World
Imagine: UK 0845 612 0094

Registered Company No. 4145 963 Registered for VAT. ISSN 1473-4362

EYE SPY 109

WHEN INTELLIGENCE COLLIDES WITH THE

UNDERWORLD



AVAILABLE LATE MAY 2017



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 page 82



Dear Newsagent, please reserve or deliver a copy of EYE SPY on publication, starting with the next available issue

NameAddress.....

Post/Zip Code

Hand the coupon in to your newsagent, or a simple handwritten note is adequate

THE ULTIMATE SPY SITES TRAVEL GUIDE OF LONDON

CLASSIFIED: THE INSIDER'S GUIDE TO 500 SPY SITES IN LONDON

*Incorporating highlights and significant moments
of over 100 Years of British Secret Service*



**SPECIAL
NEW PRICE!
EXTENDED
2017**

"A fantastic adventure in time"

Former MI6 Fort Monckton trainer



UK £22.50 USA \$32.00 WORLD £25.00

PRICE INCLUDES P&P/AIR MAIL

Orders despatched in 24 hours!



- Full colour throughout
- Large format • 544 pages
- Complete street index
- Over 1,900 photographs
- 1,000 commissioned images

- intelligence service headquarters • branch locations • operations' and planning centres • watcher surveillance residences • front companies
- interrogation rooms • special spy training schools • equipment centres
- spy and spy chief residences • branch locations • dead letter drops
- covert agent meeting points • safe houses • notorious spy residences
- spy recruitment locations • entertainment and clubs • codebreaking buildings • assassins • garages and lock-ups • honeytraps • plots
- disguises • strange twists of fate • heroes • villains

To order use form on page 82 or via Internet -
<http://www.eyespymag.com/500-book.html>

OR TELEPHONE EYE SPY DIRECT: 01756 770199 UK
TOLL FREE: 877 309 9243 NORTH AMERICA