

THE COVERT WORLD OF ESPIONAGE

EYE SPY



NUMBER 113 2018

£3.95

THE DARK WEB

AN INTELLIGENCE PERSPECTIVE

CYBER SEAS

HACKING & ESPIONAGE FEARS

Communication Tradecraft

TOP SECRET

JERUSALEM

OPENING
PANDORA'S BOX?

THE 30% SOLUTION

TRUMP, MI6 AND THE FBI

Printed and Published in Great Britain



An Intelligence Perspective

36

DARK WEB

An insightful intelligence overview of the most dangerous areas of the so-called Dark Web

Collusion, Dirty Tricks & Covert Liaisons

48

THE 30% SOLUTION

MI6 officer who wrote the 'Trump Dossier' concedes some of its explosive content may not be accurate...

THE LIVES OF OTHERS



SOE
Exploding
Rats and WWII
Assassins
Tools



61

CYBER SEAS & CONTROL

Hackers and rogue traders seek maritime targets

15



COMMUNICATION & ESPIONAGE ADVENTURE IN TIME

Nazi Germany's quest for the atomic bomb

OUT OF TIME THE SPY WHO SAVED THE WORLD

56

UK EYES ONLY

22

NEW THREATS TO THE DEFENCE OF THE REALM

10 NEW SERIES COMMUNICATION METHODS

70

↑ Arrivals
Baggage reclaim

EYE SPY 113



VOLUME XV NUMBER ONE 2018 (ISSUE 113)
ISSN 1364 8446 publication date: JANUARY 2018
FRONT COVER MAIN IMAGE: TALISMAN INTEL LIBRARY

Established December 2000



MAJOR CONTENT GUIDE

- 4 ST. PETERSBURG PLOT**
CIA intelligence on ISIS cell helps Russia foil a major New Year's Eve terrorist attack - Putin thanks Trump
- 8 MOSSAD INSIDER**
Iran sentences to death alleged Mossad agent who provided details on a number of assassinated nuclear scientists
- 10 MOSCOW'S FAVOURITE MI6 SPY**
British Cold War traitor George Blake heaps praise on today's Russian spies as he nears his 100th birthday
- 15 CYBER SEAS**
Intelligence concerns as cyber hackers and criminals focus on maritime operations, vessels and port cargo
- 20 INTELLIGENCE COLLECTION**
Russia launches new wave of intelligence operations on NATO's eastern flanks as suspected agents detained
- 22 UK EYES ONLY**
British Intelligence initiate counter-terrorist programmes to combat increasing threat of ISIS attacks
- 33 OPENING PANDORA'S BOX**
As America recognises Jerusalem as Israel's capital, intelligence and security officials warn of dire consequences
- 42 THE SUBWAY BOMBER**
US Intelligence warns of continuing ISIS lone wolf threat as terrorist attempts to cause more carnage in New York
- 44 UNIVERSAL EXPORTS**
Middle East intelligence agencies secure evidence that Iran is arming terrorist factions in Yemen and elsewhere
- 46 SECRET DAESH ACCORD**
CIA concerns as hundreds of ISIS terrorists secure their freedom after being given an escape corridor out of Raqqa
- 51 DOCUMENTS AND AN MI6 SLUSH FUND**
Released intelligence files on various British operations, including a 'private' fund for a famous MI6 official
- 56 OUT OF TIME**
A fascinating step back in time as Eye Spy examines the secret SOE operations enabled to thwart Nazi Germany's quest for the atomic bomb
- 66 COMMAND AND CONTROL**
FBI concerns as President Trump publicly criticises America's premier domestic counter-intelligence organisation
- 70 10 - COMMUNICATION TRADECRAFT**
NEW SERIES - Eye Spy looks at 10 secret methods of communications used by past and present spies
- 78 THE ADVENTURER**
One of life's great intelligence adventurers and friend of Eye Spy, Captain Leonard LeSchack, sadly passed away shortly before Christmas 2017. A look-back at his splendid career

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

"Things the president has put on his Twitter account actually have a real-world impact on our capacity to understand what's going on in other places in the world..."

Director CIA Mike Pompeo



FIRST WORD: EDITORIAL

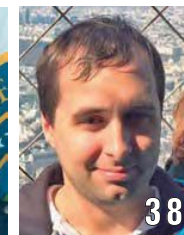
2018 INTEL FOCUS: CHINA'S SPIES AND IRAN



I recall almost two decades ago walking through London's energetic China Town region with a former MI5 agent who insisted that China has the world's greatest spying mechanism in respect of HUMINT (Human Intelligence). "No country in the world can match its prowess in terms of former nationals willing to engage in espionage for the motherland," he said. His words have long been echoed by spymasters in the USA and UK. Technology and secrets have been secured by China's spies evidenced by the duplication of warplanes, warships, control systems and space technology bearing a remarkable similarity to that produced in the West. And in recent weeks, Germany and Australia have warned of Beijing's burgeoning spy empire which seems somehow shielded to countermeasures.

Another country that continues to be watched by the intelligence world is Iran. Recent protests against the government were quickly dismantled by blocking social media and various communications tools - and a blanket ban was imposed on media outlets which were ordered not to report on demonstrations. Whilst the ploy seemingly worked, Iran could not hide a most clever and covert operation to send weaponry to militant and terrorist factions elsewhere in the Middle East and parts of northern Africa. Intelligence collectors from several countries have secured physical evidence that weaponry is being exported by Iranian factories to the groups. These stories and more, including the sentencing of a Mossad agent who allegedly identified a number of key Iranian scientists assassinated a short time ago, continue to make Iran a key intelligence target.

MARK BIRDSALL, MANAGING EDITOR



H E A D L I N E R S



- 8 Ahmadreza Djalali •10 George Blake •34 Michael Hayden
- 38 Alexandre Cazes •42 Slobodan Praljak •48 Christopher Steele
- 55 Christine Keeler •78 Leonard LeSchack

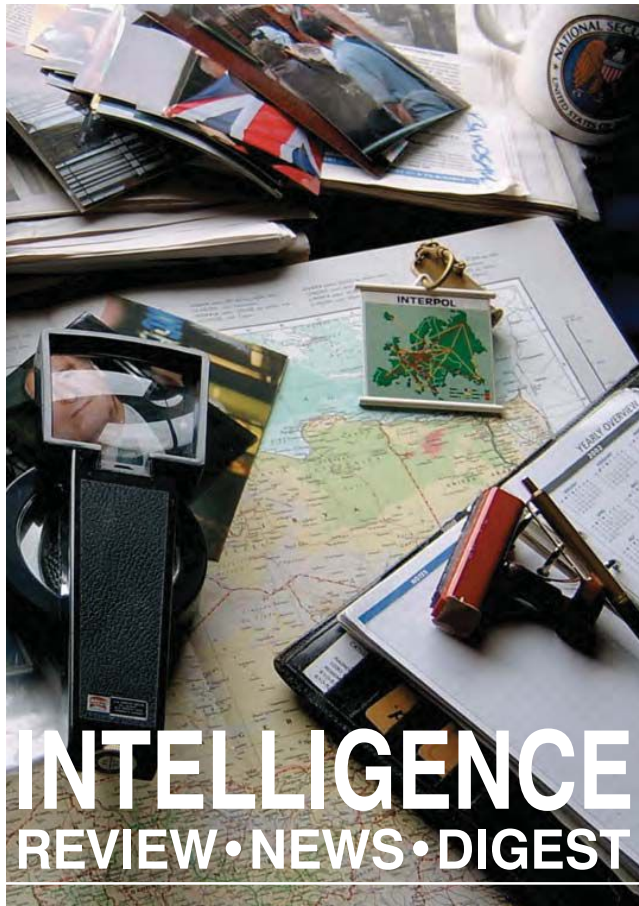
I N T E L L I G E N C E C H O I C E

THE DARK WEB - AN INTELLIGENCE PERSPECTIVE

In recent weeks there has been much discussion about an area of the Internet called the Dark Web (just one of a number of descriptions). From the moving of monies to the illegal purchase of weapons, drugs and even the hiring of contracted assassins, this murky and seemingly impenetrable area has come under much scrutiny by the intelligence world. And let's not forget its use by the spying community; as a key communication tool and payment system for those willing to engage in the world's second oldest profession, it is proving more than useful.

In this edition cyber specialist Kevin Coleman engages on a journey revealing and explaining in simplistic and chilling terms, its function, uses and users, and why it's best to avoid its darkest corridors.

•36 THE DARK WEB



INTELLIGENCE REVIEW • NEWS • DIGEST

INTEL EXPERIENCE

SPIES STEPPING BACK INTO THE FRAY

Intelligence sources claim around 300 retired intelligence operators, including some 70 MI6 personnel and 200 from GCHQ have been rehired by their former respective agencies. The decision was reportedly taken to help the UK agencies tackle increasing threats to security. However, the move has been questioned by some observers who note all three major agencies, MI6, MI5 and GCHQ, are in the midst of securing new staffers in on-going recruitment drives.

Another contentious point is that several of the senior spies now back in service, are said to have received redundancy packages worth around £100,000.

However, the move mirrors recent events in America where agencies



such as the CIA, are now inviting experienced staffers to return (some part time) to help support operations and pass on vital experience to new recruits.

- Documents related to the funding of British Intelligence in the past 12 months, show a little over £1 billion (\$1.3 billion) was spent on outside contractors.

MOSCOW'S INSIDE MAN?

Ukraine Intelligence Arrest Alleged Russian Spy Who Visited Downing Street and White House

Counter-espionage officers from Ukraine's SBU intelligence service, have detained a senior interpreter acting for some of the country's most prominent government officials. Stanislav Yezhov, 39, has been accused by Prime Minister

Volodymyr Groysman of "acting on behalf of the interests of a hostile state for a long time." Intelligence sources are satisfied that Russia's SVR was his controlling agency, indeed, Groysman himself publicly stated as such when asked which country was involved.

Interestingly, Yezhov was part of a Ukrainian Government delegation which visited Downing Street in the summer of 2017. It is believed intelligence people were present during that meeting. British officials have been reluctant to enter the debate on Yezhov. When asked about his alleged spying activities, Prime Minister Theresa May said: "I am aware of the reports in respect of a Ukrainian national who attended Downing Street earlier in the summer." Foreign Secretary Boris Johnson said: "I think the matter is one for the Ukrainians to deal with," this



Volodymyr Groysman

after he was asked if he would raise the subject during a planned meeting with Russian Foreign Minister Sergei Lavrov.

The SBU searched various addresses and offices linked to Yezhov and allegedly removed



Yezhov (circled) with Theresa May and Volodymyr Groysman at Downing Street



ST. PETERSBURG

ISIS NEW YEAR'S EVE PLOT FOILED

Russia's FSB has foiled two advanced bomb plots in the city of St. Petersburg - one to coincide with New Year's celebrations, the other targeting the city's famous Kazan Cathedral. Seven suspects were

detained and both plots involved the use of suicide bombers.

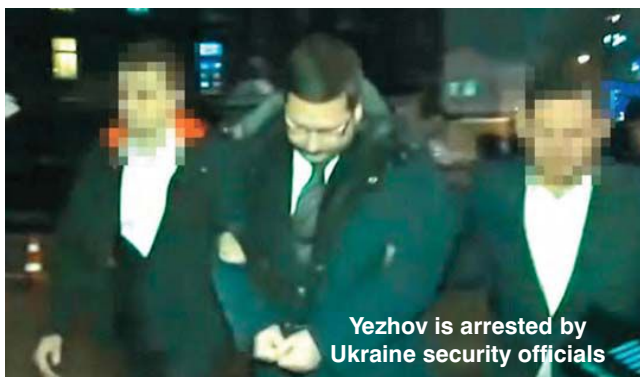
One of those arrested, 18-year-old Evgeny Efimov told investigators: "I was supposed to make the explosives and pack them into bottles and other projectiles. My task was to perform a terrorist act in the city of St. Petersburg."

Video released by the FSB shows investigative officers raiding a shipping container which was used to store and manufacture explosives. Assault weapons and ISIS literature were also recovered. Two suspects were detained.

Intelligence officials said the cell was "being directed by an



New Year's Eve target - Kazan Cathedral



Yezhov is arrested by Ukraine security officials

equipment said to be connected to his spying activities. "He acted to collect information on the government and passed this on via electronic channels of communication," an SBU spokesperson said. However, though the SBU has opened a treason case, no formal charges have yet been made.

For the record, Yezhov has acted as an interpreter at various high-profile events: in 2016 he attended

a meeting between premier Groysman and then US Vice President Joe Biden; in October 2017, a meeting between Canadian premier Justin Trudeau in Ottawa on possible weapons sales to Ukraine.

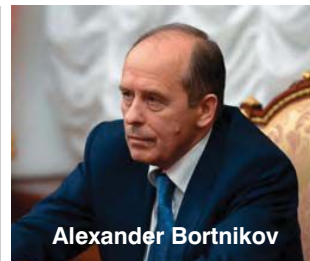
• In recent times, both MI6 and the CIA have strengthened relations with the SBU in respect of information sharing - this to counter Russian intelligence activity in the Ukraine.



FSB CT specialists raid safe house and detain suspected ISIS cell members

overseas ISIS controller using the encrypted Telegram messenger app." The communications provider has been embroiled in a bitter battle with the FSB over privacy concerns, including its refusal to hand over voice data related to two suspects linked to the April 2017 Metro bombing in which 14 people died.

FSB Director Alexander Bortnikov held a meeting with senior officials from the National Anti-Terrorism Committee. He warned that following the defeat of ISIS in



Alexander Bortnikov

Syria, many of its Russian-based supporters are now returning home. "They are planning terrorist attacks including some to disrupt the 2018 presidential election," he said.

CIA INTEL HELPED THWART PLOTS

In an unusually open and candid public exchange, President Putin telephoned President Trump to thank the CIA for providing intelligence on the cell which planned the St. Petersburg operation. The call was confirmed by press officers in Moscow and Washington.

"Based on the information the United States provided, Russian authorities were able to capture the terrorists just prior to the attack that could have killed large numbers of people," a Whitehouse spokesper-

son said. "Both leaders agreed that this serves as an example of the positive things that can occur when our countries work together."

Interestingly, Russian media first reported that the latest ISIS plots were discovered after the owner of a garage - rented out to Efimov - became suspicious about his activities and reported his concerns to police.

• The FSB announced that it had foiled "17 major plots by ISIS in 2017."



An ISIS suspect is arrested

Turkey Coup d'état

Media Attempts to Draw CIA into Failed 2016 Operation

Repercussions following the 2016 coup attempt in Turkey continue, and now a former CIA officer has become the latest intelligence figure caught up in its aftermath. Legal officials in Istanbul's Prosecutor Office have issued an arrest warrant for Graham Fuller, former Vice Chairman of the National Council at the CIA, accusing him of "violating Turkey's constitution, attempting to overthrow the government and obtaining classified documents for espionage purposes." News media in Turkey allege he had links to the Fethullah organisation

(FETO), designated a terrorist group which the government claims led the coup.

The charges seem linked to earlier accusations blaming US-based cleric Fethullah Gulen of being the 'prime mover' behind the bloody events. He has vehemently denied any involvement.

Part of Turkey's enormous post-coup investigation, which has already seen over 100,000 people linked to the operation lose their jobs and thousands jailed, has also referenced two other US-based figures, American national



Grand National Assembly building in Ankara following the failed 2016 coup

Henri Barkey, an academic, and former Turkey opposition lawmaker Aykan Erdemir. One media house called Barkey a "former CIA employee" and that he met Fuller in the Palace Hotel in Istanbul in July 2016 - shortly before the coup. Gulen was allegedly discussed.

However, it soon transpired that at the time in question, Fuller was speaking to a group of 100 people in Canada.

Asked about the alleged 'liaison', he dismissed the false stories, stating that he has not been in Turkey for five years and that he met Gulen only once... 15-years ago. However, he acknowledged why Turkey is suspicious because of previous US Government



practices, but said claims of CIA involvement in Turkey's coup which he described as "pathetic, ill-conceived and amateurish," were wrong.

Turkey continues to claim Gulen is head of the 'FETO terrorist group'.



Graham Fuller and Fethullah Gulen

LEAKS & WHISTLEBLOWERS

New Australian Spy Legislation

Australian Prime Minister Malcolm Turnbull has announced new legislation that will ban foreign political donations which could be used to manipulate aspects of government. "Foreign powers are making unprecedented and increasingly sophisticated attempts to influence the political process," he said.

The new laws come amidst major spying concerns that Chinese Intelligence are attempting to infiltrate the higher echelons of government, and follow proposed secrecy legislation intended to target government and intelligence

whistleblowers and perhaps even journalists. All those convicted could now face up to 20 years in jail for disclosing classified information.

The secrecy law, which if passed could be introduced as early as July 2018, now applies to anyone, (including serving and retired intelligence people). Human rights' watchers warn they could easily apply to journalists and organisations like WikiLeaks that 'communicate' or 'deal' with information. They will also close a long-standing gap around contractors working on behalf of government agencies, who will



2017. Prime Minister Malcolm Turnbull (left) with US Admiral Harry Harris and Joint Chiefs of Staff General Joseph Dunford

also be subject to the new offences.

EDITOR'S NOTE: Journalists will continue to have some protection if publication of information is considered to be in the public interest and is 'in the person's

capacity as a journalist engaged in fair and accurate reporting'. It is my understanding they are broadly similar to those already functioning in the UK. Nevertheless, if charged, a journalist will still have to prove they acted in the aforesaid manner.

INFILTRATION AGENTS

CIA and Mossad Blamed for Iran Government Protests

Iran has blamed infiltration agents from the CIA and Mossad for organising a spate of anti-government demonstrations in the country which began on 28 December 2017 in Mashad. Initially events focussed on economic policies, but attention soon turned to the country's leadership and the capital Tehran. Around 20 people died, and over 1,000 were arrested at various events which called for the overthrow of the government. Two police officers also died in numerous violent clashes.

Iranian Intelligence blocked social media apps to thwart supporters organising further events,



Anti-government protests were held throughout Iran

including exchanging imagery of the rallies. Internet usage was also affected with a 50% drop in

services, whilst Instagram was temporarily blocked. Interior Minister Abdolreza Rahmani Fazli



Abdolreza Rahmani Fazli

blamed "improper use of social media" saying it was "causing violence and fear." Interestingly, state media were banned from covering the protests.

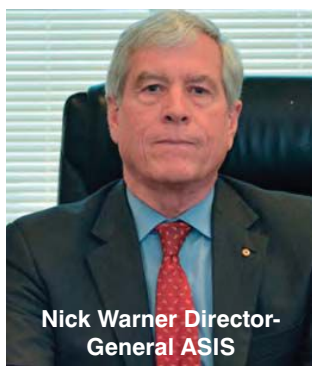
In Tehran, government officials said the CIA and Mossad were behind the trouble, which allegedly included attempts to occupy government and military buildings. The allegations were not supported by any evidence.

ASIS RECRUITMENT DRIVE

Spy Agency Eyes New Talent

The Australian Secret Intelligence Service (ASIS) said it is looking to diversify its candidate pool. Foreign Minister Julie Bishop said the organisation is recruiting people who are "smart, perceptive and empathetic..." the same skills required by those in the teaching and customer service professions.

"What we are looking for is people from a diverse range of backgrounds. People who have got a curious outlook, who are



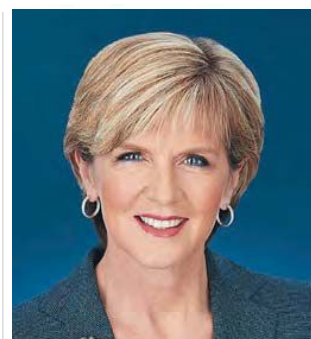
Nick Warner Director-General ASIS

obviously intelligent - it's an intelligence service," Bishop said

whilst promoting the recruitment drive. "People who are observant, bright, able to form relationships. Be prepared to be deployed overseas and act in Australia's national interest."

Applicants using the Service's website are asked to take part in an online game where they are tested on their abilities to notice small details, read faces and assess the reliability of information.

The job advert uses the tagline 'Be part of more human, human intelligence'. ASIS is looking for those who 'are highly motivated, have an innate sense of curiosity and a love of travel to reach



Foreign Minister Julie Bishop

outcomes that have the potential to save Australian lives'.

The selection process reportedly takes approximately seven months - a figure comparative to MI6, for example.

OPENING INTELLIGENCE DOORS

FSB to Participate in New Television Series

Intelligence sources in Moscow have confirmed that Russia's Federal Security Service (FSB) is set to participate in a series of television shows and documentaries, highlighting 100-years of secret service in Russia.

The FSB's Public Board released a statement saying that it will

cooperate with state media houses focussing on the current and past work of intelligence services in Russia - the objective being to provide an insightful overview.

FSB PB Chairman Vasily Titov said: "Undoubtedly we should pay more attention to countering attempts to distort history,



© TASS ARCHIVE

particularly that of the special services, as well as diminish their role in distorting history. Their century-long history includes many heroic pages, some written

with the blood of their officers who fulfilled their duties until the very end, both in times of war and peace."

MOSSAD NUCLEAR 'SPY'

SCHOLAR'S DEATH SENTENCE UPHELD IN IRAN

Dr Ahmadreza Djalali, an Iranian-born Swedish resident and specialist in emergency medicine, who was arrested during a trip to Iran in April 2016, has been told by the court that his execution will go ahead because no appeal was submitted before a designated deadline. Dr Djalali was accused of passing information to Israel's Mossad intelligence service during negotiations that led to Iran's nuclear deal with world powers in 2015.

Amnesty International said the Supreme Court in Iran upheld his death sentence in a summary manner without granting defence lawyers an opportunity to file submissions.

According to statements by the international Committee of Concerned Scientists (CCS) and

Scholars at Risk (SAR), before Djalali was convicted, his solicitor was dismissed and a defence solicitor appointed on instruction of the court. A time delay then ensued and his family discovered that no appeal was submitted. As a 20-day ruling on submissions passed, the sentence now stands.

Djalali, who teaches disaster medicine at universities in Italy and Belgium, was arrested while visiting Iran to participate in a series of academic workshops. He was accused of "collaborating with the enemy state," tortured, and was asked to spy for Iran but refused, according to CCS sources. Translation of a note written by Djalali inside Evin Prison, and circulated by a close contact, indicates Djalali believes he was arrested for refusing to spy for Iran's Ministry of Intelligence (MOI).



PROFILE: DR AHMADREZA DJALALI is a medical doctor and lecturer at the Stockholm Medical University, Karolinska Institute, Sweden, and a research associate in disaster medicine at the Centre for Research and Education in Emergency and Disaster Medicine at the University of Eastern Piedmont in Novara, Italy. He also teaches at the Vrije Universiteit Brussel in Brussels, Belgium.

THE FO JOURNEY MAN

Foreign Secretary Presses Iran to Release UK National

Britain's Foreign Secretary Boris Johnson travelled to Iran in a bid to help secure the release of UK national Nazanin Zaghari-Ratcliffe, 37. She was arrested in April 2016 by officers of the Iranian Revolutionary Guard whilst visiting relatives in Iran. Ministry of Intelligence officials accused her of spying, and involvement in a plot to topple the regime, charges ridiculed by most intelligence watchers.



Nazanin and Richard with daughter Gabriella



Boris Johnson



Mahmoud Alavi Director of Ministry of Intelligence

Her case was somewhat complicated by Mr Johnson himself, who just weeks earlier said she was "teaching journalists in the country."

The remark was seized upon by Iranian Intelligence because in October 2017, the Prosecutor General in Tehran said part of the charge against Zaghari-Ratcliffe related to her alleged involvement in an on-line BBC Persian* journalist course. Iran believes this endeavour involves training and recruiting journalists who would then engage in propaganda against the country. Iran continues

to reference her work for the BBC World Service Trust.

Asked if he thought his visit had been successful, Mr Johnson said: "It was worthwhile, but I don't want to raise false hope. It's too early to be confident of the outcome."

Nazanin's husband, Richard said: "I wasn't presuming that she would come back on the plane with him [Johnson]. It was always the best case scenario that his going would unlock the door and then days later she might be able to come home."

فارسی BBC

INTEL INSIDE

*BBC Persian Television, launched in 2009, has the potential to reach over 100 million people and is focussed on the Persian-speaking countries of Iran, Afghanistan, Tajikistan and Uzbekistan. In 2017, Iranian Intelligence seized the [Iranian] assets of 150 contributors. In the past three years, there have been a number of suspected attempts by the MOI to jam the signal of the station.

BENGHAZI MISSION TRIAL

ATTACK SUSPECT GUILTY OF OPERATIONAL CONTROL

Ahmed Abu Khattala, 46, the man charged with various terrorist crimes in connection to the 2012 storming of the US Consulate and CIA compound in Benghazi, Libya,



Ahmed Abu Khattala following his capture in June 2014 by US Special Forces

has been found not guilty in a US court of the most serious charge – murder. However, he has been found guilty of four other terrorist charges, some of which carry a lengthy prison sentence. And despite the lesser charge, prosecutor Michael DiLorenzo had argued that Khattala was a “stone-cold terrorist... who attacked mission facilities and was there to kill Americans.”

The jury found that Khattala, whilst not directly involved (physically) in the killing of Ambassador Christopher Stevens, information officer Sean Smith, CIA contractors and former US Navy Seals Tyrone Woods and Glen Doherty, was instrumental in the planning and orchestration of the attacks. Evidence showed he had directed operatives using cell phone communications and had thwarted efforts by emergency

services and other US-supportive militias to reach the attack zones.

Acting Assistant Attorney General for National Security Dana Boente said: “Our work is not done. We will not rest in our pursuit of the others who attacked our facilities and killed four courageous



Dana Boente

Americans who perished that day.” Another attack suspect, Mustafa al-Imam, was captured

in 2017 and will also face trial. Following the verdict, CIA Director Mike Pompeo told staffers at Langley: “A small measure of justice was meted out.”



PANAMA Assassination PAPERS

VALLETTA: Three men have been charged in connection with the car-bomb murder of Maltese investigative journalist Daphne Caruana Galizia (see Eye Spy 112).

Galizia focused her research on corruption, drug trafficking and scandals involving Malta's elite and wrote about links to offshore financial havens in Panama and elsewhere.

The killing of Galizia, using a remote-controlled IED, shocked the island nation and led to the European Parliament sending a delegation on a fact-finding mission related to the rule of law in Malta. The EU delegation expressed concerns and issued a warning that the “perception of impunity in Malta cannot continue.”

The investigation into her death was assisted by the FBI, Europol and Finland's National Bureau of Investigation. The FBI used equipment to collect “electronic communication evidence” that led to the suspects; including triangulation data of the call that triggered the bomb that killed Galizia.

The three suspects in custody all had previous criminal records. Two of them, Vincent Muscat, 55, and Alfred Degiorgio, 52, nicknamed il-Fulu, were acquitted in 2004 on armed robbery charges while Degiorgio's brother George, 54, nicknamed ic-Ciniz, was charged with possession of unlicensed weapons and tools used to pick locks.



Daphne Caruana Galizia

THE LIGHTER SIDE

Russian farmer faces fine and jail for spying... on his cow

Yevgeny Vasiliev, 39, a farmer from the village of Lopatki in Russia's Kurgan region faces a spell in prison or a fine, for buying a GPS tracker from China to ‘spy’ on... his cow. The farmer, who suffers from asthma, wanted to make it easier to find the animal as it moved across fields.

Mr Vasiliev bought the device from China's AliExpress which cost him 390 rubles (£5.50) at the beginning of 2017. After waiting months, he received the parcel in September but did not realise that under Russian law, at this very

moment he became a ‘spy’; the GPS tracker, it transpired, had a small microphone, which can allegedly be turned on remotely. These devices are outlawed in Russia, but he had no idea that he was buying something illegal, for its description, written in poor Russian, failed to mention the microphone.

Incredibly, as soon as Vasiliev left the post office with his package, officers from the FSB detained him. “When I received the tracker



Yevgeny Vasiliev



and exited the building, the FSB servicemen approached,” said Vasiliev. He was notified his purchase was illegal and asked for an explanation.

With nothing to hide, he showed the officers his computer and his on-line order. Vasiliev explained that he had intended to use the device to keep track of a wandering cow. Not satisfied, the FSB charged him for acquiring ‘special technical equipment for sourcing unofficial information’. If found guilty, he could face a fine of up to 200,000 rubles (£3,000) or four years in jail.

Vasiliev told journalists: “But who can I wiretap in the village?” He went on to say that the device would need a SIM card (which he could not afford) and doubted he could even get reception.

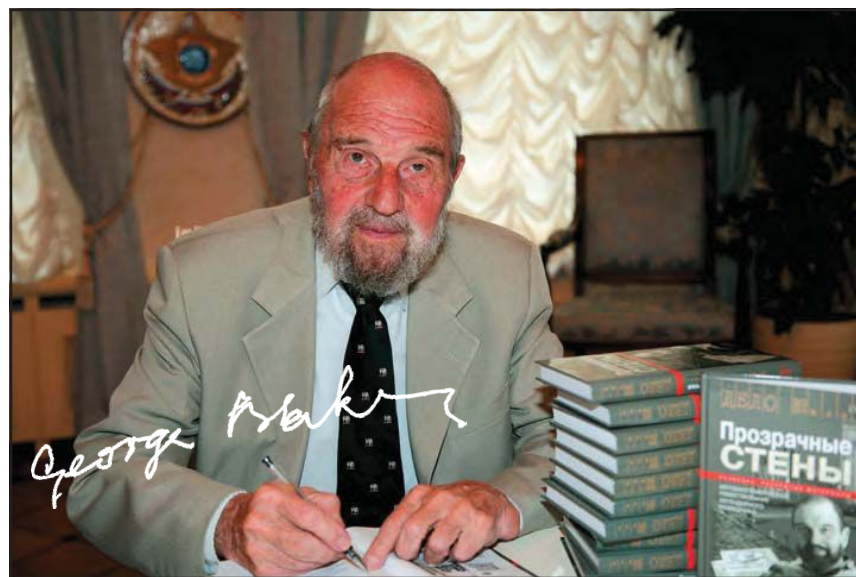
DOUBLE AGENT HAILED BY SVR NO REGRETS

COMRADES AND COMPATRIOTS: RUSSIAN INTELLIGENCE PROGRAMME CONTINUES TO ENGAGE WITH PUBLIC

On the occasion of his 95th birthday, former MI6 officer and KGB spy, George Blake, reiterated his support for Russia's burgeoning intelligence services, especially in the growing area of counter-terrorism, a subject he rarely encountered whilst operating as a double agent for Moscow. Speaking from his residence on the outskirts of Moscow, he said Russia's spies have the "difficult and critical mission of saving the world... terrorism has left bloody traces in many corners of the world. It's a true battle of good and evil."

Blake took a sideswipe at North Korea and the West saying Russia's SVR (Foreign Intelligence Service) must "save the world... in a situation when the danger of nuclear war and resulting self-destruction of humankind has again been put on the agenda by irresponsible politicians." He referred to SVR officers as "comrades and compatriots" and Russia as the "motherland." Deliberate words drawn from his experiences in the secret spy wars of the East and West. He heaped much praise on today's Russian Intelligence system noting it had supported him throughout his half-century of time living in the country.

In recent weeks, President Putin has moved to 'showcase' the important work of the



George Blake signs copies of his book - note SVR shield in background

intelligence services and why the public should back agencies and their spies. Exhibitions and special television programmes have highlighted some well and less known spies, revealing the "heroic work for the motherland," as one Moscow newspaper editor said. Special attention was paid to the work of MI6 officer Kim Philby who defected to Russia at the height of the Cold War (See

Eye Spy 112). SVR Director Sergei Naryshkin hailed Philby's achievements and also praised Blake saying the intelligence man had been a "role model for the agency's officers."

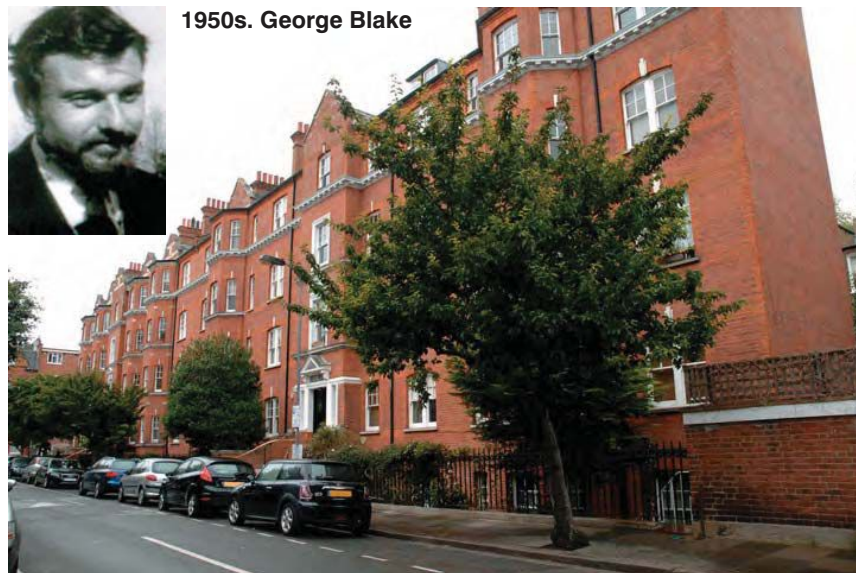
Described by *Sputnik News* as a 'renowned and legendary Soviet intelligence officer', Blake congratulated serving spies and gave backing to Russians currently considering a life in the shadows. "I believe in you, in your unselfish sacrificing service of our common goal... in your professionalism," he said. "I believe in the final victory over the villainous

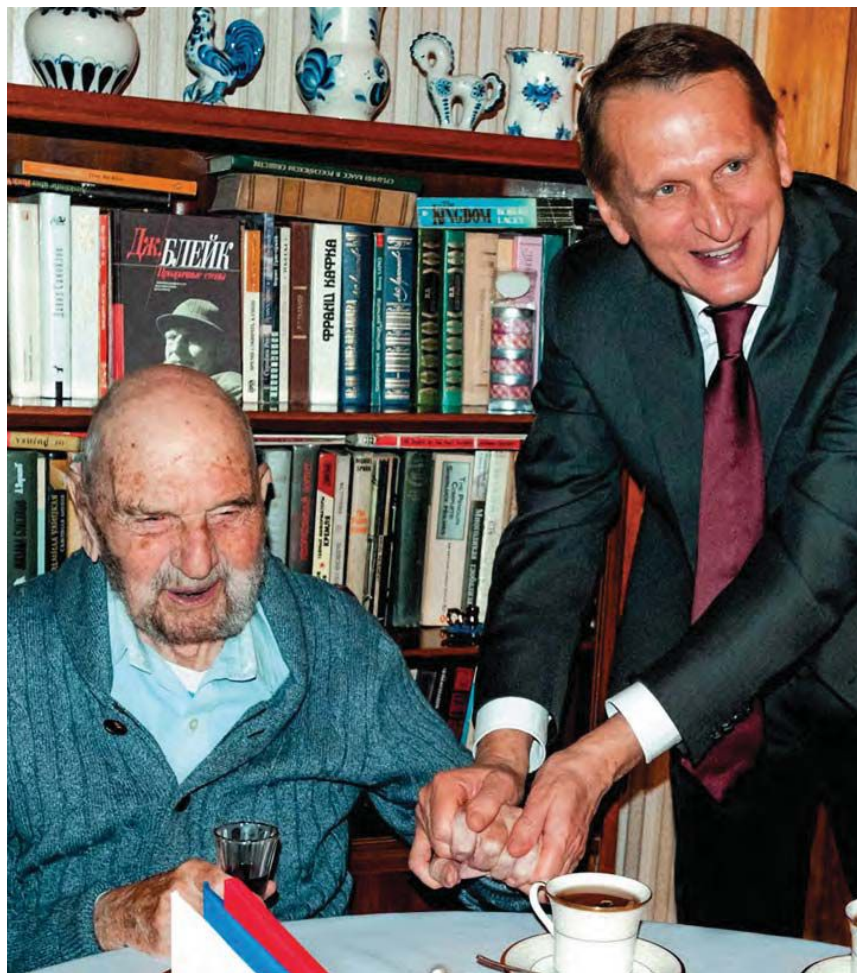
MI6-CIA OPERATION GOLD

INTEL INSIDE MI6 officer George Blake was tasked with taking notes of the MI6-CIA meeting discussing the Berlin spy tunnel project. Just two hours after the October 1953 briefing, he duly deposited them into the hands of his KGB handler. Thereafter he made the short journey to the apartment (left) of his mother in this London building where he often stayed. She cooked supper and the two watched television and conversed. Blake admitted that he "cared not one jot," about his betrayal of British and American secrets.



1950s. George Blake





SVR Director Sergei Naryshkin with George Blake as the double agent celebrates his 95th birthday

enemy and this belief gives me the power to live on." He failed to identify the 'enemy' on this occasion.

Dutch-born Blake began operating for British Intelligence in 1944 and is best remembered for betraying secrets to the KGB of the joint CIA-MI6 Cold War spy tunnel operation in Berlin. In 1961 he was betrayed by a KGB officer working for British Intelligence and sentenced to 42-years in prison. He escaped from Wormwood Scrubs Prison in 1966 and fled to Moscow where he has resided ever since.

In 2012, on reaching his 90th birthday, he joked to reporters that he once told a gathering of Russian intelligence officers that he had "enjoyed life in Russia," and compared his transition to a "foreign-made car that had adapted well to Russian roads." Five years on Blake said he does not regret anything from his past and looks forward to the future with optimism.

British Intelligence has released materials which show Blake was responsible for leaking the identities of MI6 spies. At least six agents were jailed in East Germany and one was almost certainly executed.

THE RUSSIAN THREAT

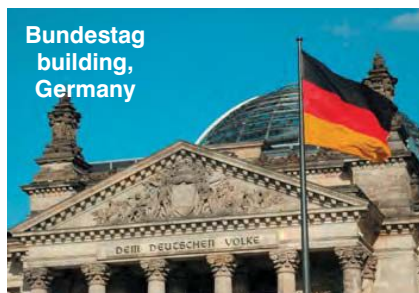
Weaponising Information

British Prime Minister Theresa May launched a vociferous attack on Russia's spy agencies accusing them of "endangering global security, election meddling, cyber hacking and spreading fake news." Armed with intelligence from MI6 and friendly overseas organisations, May said that Moscow was behind cyber breaches within offices of Denmark's Ministry of Defence and Germany's Bundestag (parliament), to name but two. *The Times of*

London described her comments as a 'lengthy charge sheet'.

The premier also referenced an increase in Russian Air Force surveillance flights which routinely breached national airspace boundaries, and its 'hidden hand' in the continuing conflict in the Ukraine. She also pointed to bogus imagery which was 'stage managed' to spread disinformation in "an attempt to sow discord in the West and undermine UK institutions."

Speaking to Russia directly, May said: "We know what you are doing... and you will not succeed. We do not want to return to the Cold War or be in a state of perpetual confrontation." She also used a phrase which is becoming commonplace in the continuing fractious relationship between the Media and Intelligence world - "weaponising information." As a caveat to her powerful attack, ➤



Bundestag building, Germany



HMS Liverpool escorts Russian aircraft carrier Admiral Kuznetsov near British territorial waters



RAF Typhoon flies alongside a Russian Bear-H warplane in the North Atlantic



Foreign Secretary Boris Johnson

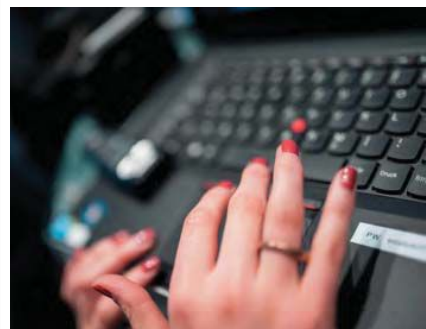
and terrorism in Europe, has had its day. You can't save it by attacking Russia."

Russia's Foreign Minister Sergei Lavrov said, "hysteria is being fuelled up in order to divert attention away from [the UK's government's] inability to solve domestic issues."

Other intelligence figures point out that just days earlier, President Trump announced that he did not believe Russia interfered with the US General Election and "believed President Putin" who has long rejected such claims. That's not how some US intelligence officials view the situation and the president somewhat confused the issue when he said "I believe our intelligence agencies."

It's more than likely May had long discussions with officials from the UK intelligence system before making her views known. And interestingly, Russian media houses focussed on statements issued by the premier just days after her attack. During questions in Parliament May said: "If they care to look at my speech they will see that the examples I gave were not in the UK."

- Britain's Electoral Commission is currently engaged in an investigation following claims (part-supported by intelligence) that some 'players' in Russia used social media as a supportive tool to convince Britons to vote to leave Europe (Brexit). Boris Johnson, whose organisation oversees the work of MI6, has already stated he has yet to see "any evidence that Russia attempted to interfere with the Brexit vote."



Adam Garrie

she said Russia could be a powerful ally "if it plays by the rules," adding that Britain's Foreign Secretary Boris Johnson would be visiting Moscow for talks.

Russia's powerful media machine, parts of which have been designated 'spy apparatus' by the CIA, naturally hit back. Managing Editor at The Duran.com, Adam Garrie, told Russia Today (RT): "The little sister of America has truly spoken." He believes her notes were an attempt to regain support from the British public in wake of a few turbulent weeks of discord within her own party.

One powerful figure involved with Russia Media policy is Senator Alexei Pushkov. He

dismissed suggests of 'meddling' and said: "The world order that suits May, with the seizure of Iraq, war in Libya, the rise of ISIS



Senator Alexei Pushkov



Prime Minister Theresa May



Cyber attacks have been reported targeting Britain's critical infrastructure - including power



INTELLIGENCE FROM CYBERSPACE

Perhaps central to Theresa May's attack on Russia, is intelligence gleaned by Britain's National Cyber Security Centre (NCSC). Throughout 2017, the organisation has identified several major cyber attacks targeting the country's critical infrastructure (energy) and communications sector, as well as leading commercial companies. Some of the attempts at disruption seem to have originated in Russia.

Ciaran Martin, head of the NCSC acknowledged the attacks, but has been reticent, for obvious reasons, to provide intimate details. In a prepared statement given at the Times Tech

Summit in London, Mr Martin said: "Russia is seeking to undermine the international system. That much is clear. I can't get into precise details of intelligence matters, but I can confirm that Russian interference [has] been seen by the NCSC."

Official figures related to the Russian attacks are open to conjecture, but since GCHQ launched the organisation in 2016, the agency has responded to nearly 600 major incidents, including the WannaCry attack that targeted National Health systems. Millions more minor cyber attacks have also been identified.

LINKS: www.ncsc.gov.uk



Ciaran Martin

ROGUE TRADER IN SECRETS

Cyber Specialists Compete in Government-Backed Challenge

Britain's search for new cyber specialists continues apace, amidst current and emerging threats. All manner of attacks on vital industries, including government offices, commerce, communication and transport have been reported in the last 12 months. It was therefore apt that this

year's government-sponsored Cyber Security Challenge final was therefore linked to the world of maritime security.

Set in the historic Trinity House, London, the 'home' of British shipping, the Masterclass final was the culmination of a year-long endeavour of nationwide events to source the very best candidates - all keen to engage in the future world of cyber security. Forty-two candidates participated in a realist three-day



event to identify the loss of secrets from fictitious shipping company - Fast Freight Ltd - to a rogue cyber-crime group called Scorpius. This outfit, the candidates were informed,





were a notorious bunch which had targeted international organisations extorting monies.

Candidates were placed in teams and their first task was to locate a secreted USB stick in London containing various data. Unfortunately for them, they were surveilled by officers of the National Crime Agency (NCA) to test their

ability to act in a secure manner and keep their objective (mission) secret. Once discovered, the information pointed them towards a new COO (Chief Operating Officer) at Fast Freight Ltd - he was soon identified as the culprit and loss of data to Scorpius. Thereafter the cyber defenders not only had to protect against cyber attacks, they were charged with sourcing sufficient information to bring about a legal case against the rogue executive.

Using a variety of specialist cyber tools provided for by industry specialists (spon-



Mark Hughes BT Security and Rob Partridge, head of BT Cyber Academy

sors), the evidence was secured. The teams then had to present their findings in a fictitious court of law in front of defence solicitors, real barristers and judges identifying how the security breach had occurred.

The candidates were scored on technical proficiencies, such as forensic analysis, incident response time, live network monitoring, communication, leadership and management.

At the end of the Challenge, the organisers, including specialists from GCHQ, chose Team Daman* as winners, and Mo Rahman, a 22-year-old computer science student as overall champion.

Mark Hughes, CEO, BT Security, said: "This year's Masterclass is very special for us at BT as we are not only supporting this exciting competition, but have been very much involved in the design of its final. It is through

Trinity House, London

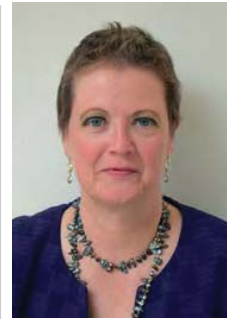




programmes like the Cyber Security Challenge that we can raise the profile of the industry and find tomorrow's cyber experts that will help us close the skills gap in the industry. BT Security protects some of the best-known brands around the world as well as the critical national infrastructure in the UK. Only by attracting the best talent can we stay ahead and keep the nation safe from cyber threats."

Paul Edmunds, head of Technical Engineering at the NCA's National Cyber Crime Unit, said: "The skills tested at the Cyber Security Challenge Masterclass have never been more vital to the UK."

The competition, created by British Telecommunications began in 2010, and interestingly,



Stephanie Daman

50% of previous Masterclass competitors now work in the cyber security industry - some no doubt with GCHQ.

*Team Daman took its name from the late Chief Executive of Cyber Challenge UK, Stephanie

Daman, who passed in June 2017, aged just 56. Her vision was to help support individuals seeking a career in cyber, especially those who do not have the means to do so.

CYBER SEAS

A Menace From Space



It's not surprising organisers of the UK Cyber Challenge chose a nautical theme for the competition. Worldwide, intelligence analysts estimate as many as 200,000 vessels are exposed to possible cyber attacks, a worrying statistic considering 90% of all trade goods are transported by sea. It's also relevant that numerous cyber attacks on shipping and maritime organisations, including military vessels have increased by 1,000% in the last decade alone.

BANGS, BUMPS AND DEATH

In August 2017, the USS John S. McCain collided with the merchant ship Alnic MC, a Liberian-flagged tanker near Singapore. Ten sailors lost their lives. Chief of Naval Operations Admiral John Richardson acknowledged his investigators were looking at a variety of causes, including the possibility the incident was the result of a cyber attack. And though the real reason, according to an official report,

appeared one of steering failure; over confidence and crew complacency, the very fact that the official even considered a cyber intrusion was revealing.

Nevertheless, others have sided toward the cyber theory, including former US Navy information warfare officer Jeff Stutzman. "When you are going through the Strait of



Surge in cyber attacks against maritime targets increase as intelligence world seeks new countermeasures



GPS antenna



Damage suffered by the USS John S. McCain



Chief of Naval Operations Admiral John Richardson

Malacca, you can't tell me that a naval destroyer doesn't have a full navigation team with look-outs on every wing and extra people on radar. There's something more than just human error going on."

A few weeks earlier in June, seven US Navy personnel died following a collision between

the USS Fitzgerald and an oil tanker east of Singapore.

For the record, in 2017, five US warships were involved in significant incidents in Asian waters, the latest occurring on 18 November. Here a Japanese tug boat apparently lost power and drifted into the USS Benfold during a towing exercise in Sagami Bay.

Following the incidents, several senior commanders were relieved of their positions or chose to step down. (See sidebar opposite)

The civilian maritime arena is regarded as being most vulnerable of course, and only now are companies waking up to the multitude of problems a cyber attack can create. Investigative files concerning incidents increasingly contain references to cyber. Case file examples are numerous: in 2015, attackers managed to 'tilt' a floating oil rig disrupting operations for 19 days; the CIA and

US Naval Intelligence discovered Somali pirates selected some maritime targets by viewing navigational displays on-line; a computer system in the Port of Antwerp was hacked allowing cyber criminals to identify the content of containers. A cyber attack was also reported by A.P. Moller-Maersk's IT system in June. Port operations were disrupted worldwide.

ATTACK BY SPACE

Interestingly, many operators are now re-examining maritime navigation security procedures; this is because investigators have confirmed cyber attacks have targeted satellite systems (GPS - Global Positioning System) used by the vast majority of major firms and vessels. Indeed, some are even considering using radio technology invented in WWII. The USA, Britain, Russia and Japan are all exploring adapted versions of the old technology to aide navigation - effectively as back-up systems. The move follows continued uncertainty if cyber hackers have played a part in the upsurge of disruption incidents related to navigation and steering.

Experts note weather systems can affect signals linking ships to satellites. And though this is an absolutely true cause of some loss of 'connection', increasingly, analysts are



Main: Damage suffered by the USS Fitzgerald is evident. Inset: Many of the US Navy's cyber elements now fall under command of Naval Information Forces



Radar display showing maritime traffic



USS John S. McCain



USS Fitzgerald



USS Lake Champlain



USS Antietam



USS Benfold

• 31 January. USS Antietam ran aground near Yokosuka Naval Base in Japan • 9 May. USS Lake Champlain collided with South Korean fishing boat • 17 June. USS Fitzgerald collided with merchant vessel near Japan • 21 August. USS John S. McCain collided with merchant vessel east of the Straits of Malacca and Singapore • 18 November. USS Benfold is struck by a tug during a towing exercise in Sagami Bay



finding alternative reasons - including cyber attacks. Examples of such happenings occurred in the summer of 2017, all coincidentally in

one location. Twenty ships complained to the US Coast Guard Navigation Center that their GPS systems had suffered disruption in the Black Sea area. Analysts suspect cyber interference - not the weather.

Freight containers at the Port of Antwerp



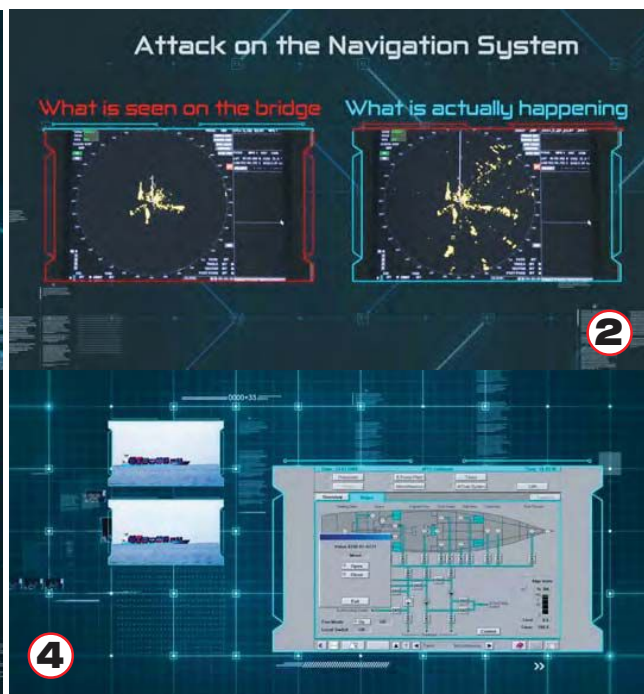
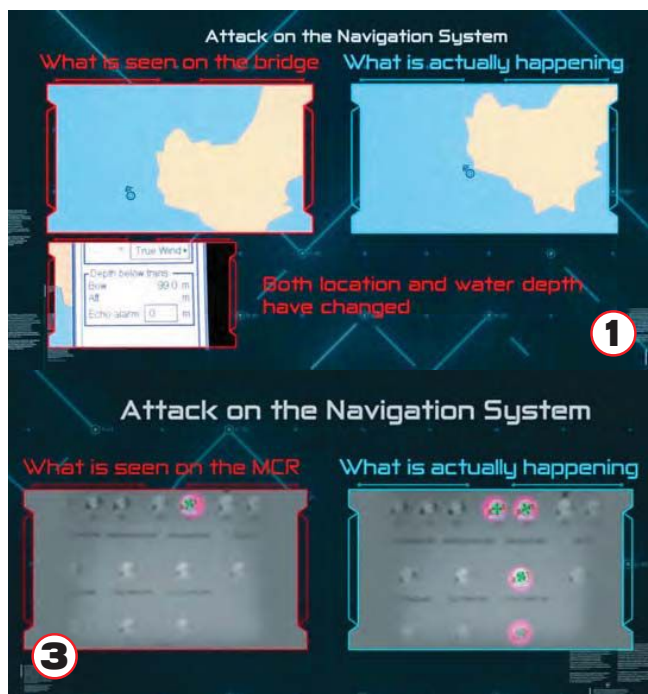
USAF GPS specialist

Cyber specialists note that Global Navigation Satellite Systems (GNSS) and GPS signals are transmitted around 12,000 miles above Earth. They acknowledge signals can be jammed by inexpensive and rudimentary

devices which are widely available. Other controlled exercises and tests involving computer systems, reveal the stark dangers. For example, using a \$3,000 antenna and an electronic GPS 'spoofer' built within a laptop computer, GPS expert Professor Todd Humphreys and his team at the University of



Todd Humphreys



1. False reading failed to show how close to land the ship really was • 2. Radar failed to show all the vessels in proximity • 3. Engine room pumps were shut down but display shows just one out of action • 4. Cyber attack on control system could have resulted in fuel spillage, pollution and caused the vessel to overturn

Texas took control of what was described as a “sophisticated navigation system” aboard a super yacht in the Mediterranean Sea.

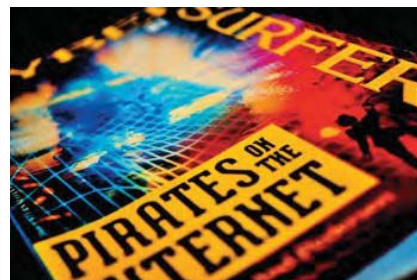
Other more adventurous and hideously clever cyber attacks against maritime organisations have also occurred. Perhaps one of the more audacious came in December 2014. A major shipping company engaged in a deal to secure a sea floor mining vessel as part of a charter contract in China. Unfortunately for them, they paid \$10 million of an \$18 million guarantee into a fictitious bank account belonging to an international cyber criminal. In 2015, a Cyprus registered shipping company received what they thought was an authentic e-mail asking to pay a client (supplier) in Africa an extra £500,000 into a different account than was previously used. Unfortunately, it was a bogus account and the entire affair was a cyber ruse. The money vanished instantly. And there are lots of other instances.

COUNTERMEASURES

Maritime cyber specialists have identified five primary areas of concern, all of which are considered vulnerable and at risk from cyber attackers:

1. Satellite Communications
2. Automatic Identification Systems
3. Ship Navigation Systems
4. Maritime Radar Systems
5. Cargo/Freight Tracking Systems

And perhaps a reflection of the growing menace and suspicion of cyber interference in the maritime world, Israel-based cyber security specialist company Naval Dome, has signed a memorandum of agreement (MOA) with Lloyds Register (LR), with a view to establishing standards and guidelines for cyber defence. As part of the liaison, LR will carry out a series of tests



on one of its vessels using Naval Dome, a multi-layered cyber defence solution specifically designed for maritime application.

The Naval Dome countermeasure has been accepted as a test platform on recommendations from senior intelligence officials. Ran Merkazy, LR Vice President said: “The company has the right credentials and an excellent understanding of the maritime





Most GPS satellites operate around 12,000 miles above Earth

intelligence sector to be able to provide the advice we need to develop concise and effective guidelines for preventing system and data security breaches at sea."

Parts of the system use cyber defence software already utilised by the world's leading intelligence agencies. Naval Dome integrates with existing systems and software providing real-time cyber alerts and blocks malicious files to prevent access to critical parts of a system.

Chief Executive of Naval Dome and former Israeli Navy Commander, Itai Sela said: "A lack of standard guidelines for creating a more secure maritime environment is the shipping industry's Achilles heel." As an example of the danger of a focussed cyber attack on a vessel, Sela said that his company had performed a series of cyber attacks on a ship's live navigation systems, engines and other machinery control systems. They were able to shift the vessel's reported position, mislead radar displays, turn on and disable machinery, override fuel control, steering and ballast systems. The rogue virus managed to enter the ship's computer system via an "innocent e-mail sent to a crew member."



Itai Sela

Once Naval Dome software was uploaded, the same cyber attack was performed. "We were unable to penetrate any of the ship's systems," said Sela.



No room for error - US warships refuel at sea



CYBER PIRATES STEERING A VESSEL FOR PROFIT

In 2017, CIA analysts examined an incident whereby cyber hackers reportedly took control of the navigation systems of a container ship enroute from Cyprus to Djibouti. According to sources, the 'pirates' had control of the ship for 10 hours and intended to steer it into an area where they would be able to board the vessel and take control for kidnap and ransom. The source, who did not want to be identified, said: "Suddenly the captain could not manoeuvre; the IT system of the vessel was completely hacked."

The crew attempted to regain control of the navigation system but had to bring IT experts aboard, who eventually managed to get them running again after hours of work. The IT team installed a specialised programme designed for the maritime industry that blocks attacks from the outside, but said the incident should serve as a warning to the industry.

Emma Biggs, business director at security brokerage firm ASKET, said: "There are vulnerabilities on all vessels. People still talk about there being a difference between what happens on board and on shore, but



Somali pirate

there isn't, particularly as now everything is connected and the telemetrics of ships are fed back to shore."

Biggs also said: "There have also been suspected cases of mass-spoofing, where the GPS systems of 20 ships were giving false locations, some inland and some at airports." Unconfirmed reports of the attacks were first posted by the US Department of Transportation's Maritime Administration (MARAD).

'Ethical hacker' Ken Munro, previously revealed hacking vulnerabilities in major maritime communications and was able to precisely pinpoint a named vessel, identify a staff member and potentially attack the ship through communication boxes aboard ships that were running outdated firmware and using default passwords.



US Navy counter-piracy specialist

RUSSIAN 'SPIES' OUTED AS NATO COUNTRIES TARGETED INTELLIGENCE COLLECTION

Spy Games Continue on Europe's Eastern and Northern Flanks

The Romanian government has expelled a suspected Russian spy banning him from the country for 15 years. Pro-Russian Serbian national Bratislav Zivkovic, 42, was accused of sourcing intelligence on various NATO bases in the southeast of the country, and obtaining classified information. Zivkovic then allegedly provided this to a Russian



Docks at Constanta Sea Port

handler though few details of the 'exchange' have been released.

Zivkovic calls himself a 'commander' of Serbia's Chetniks, a paramilitary force which fought alongside pro-Russia forces in the 2014 annexation of Crimea. He was identified again by intelligence agencies operating in eastern Ukraine with similar pro-Russian fighters. He is known to the CIA and MI6.

His activities in Romania were viewed with concern by NATO, as he is alleged to have shown much interest in securing a variety of documents on troop deployment, military objectives and of the country's critical infrastructure. Romanian Intelligence (SRI) spokesman Ovidiu Marincea said agents had exposed his activities before he could "gather any classified information." However, he posed an ongoing risk thus a decision was



Complete with medals - Bratislav Zivkovic hardly reflects the archetypal image of a spy - but his activities were a 'menace' to Romanian Intelligence and a danger to NATO

made to label him a 'spy' and ban him from entering the country.

MKAB ROMANIA

Though much information remains classified about his activities, Zivkovic is said to have visited the country on four occasions in 2017, each time journeying to the strategically important Black Sea port of Constanta.



Zivkovic in Romania



Zivkovic with associates in Eastern Ukraine

British Army Rapier Defence System deployed in Estonia. The weaponry provides air defence against aircraft, helicopters, UAVs and cruise missiles





Romanian SRI intelligence service officers attached to its special counter-terrorism element train with US Marines



Bratislav Zivkovic pictured with weaponry

noticed by Russia, and has “made itself a target which would be neutralised if confrontation happened,” he said. Zivkovic also paid much attention to mobile defence systems facing the Russian border.

As for Zivkovic, he states that Romania’s SRI has no evidence against him, “otherwise they would have charged me,” he said.

Romania is a sponsor nation of the recently opened NATO Counter Intelligence Centre of Excellence in Poland. (See Eye Spy 112).



Vladimir Evseev

Evseev, Director of the Center for Public Policy and Military Research in Moscow warned the base and its activities have already been

SUSPECTED FSB CYBER SPY ARRESTED IN ESTONIA

Unbeknown to him, he was surveilled whilst photographing military radar installations and securing their GPS positions. “He also showed interest in the Mihail Kogalniceanu military base (M.K. Air Base),” a source said. This facility is used by NATO aircraft and as a host point for US Armed Forces. It is regarded as a vital defence and logistics position of NATO forces in the Baltic Sea area and a transit route for various forces, including the famous 101st Airborne Division which arrived in 2014. It is very close to the port of Constanta. Vladimir

Estonia’s Internal Security Service (ISS) detained a suspected FSB spy as he prepared to leave the country from the border town of Narva. Alexei Vasilyev, 20, was formally charged with committing various offences linked to espionage, including preparing to “launch a cyber crime” against the country. “The target of his action was the Estonian state authorities,” a prosecutor said. Intelligence sources suspect the incident could be linked to new microchip upgrades on around 800,000 identify cards.

Estonia was a part of the Soviet Union until 1991; now it is a key Baltic member of NATO. Relations with Moscow have become increasingly strained, and there has been a gradual military build-up of opposing forces in the region, with Britain having deployed around 1,000 troops.

In the summer of 2017, Estonia designated two Russian diplomats ‘persona non grata’ and the men were expelled. This followed “inappropriate contact with key government officials.” At the same time, a third man (Russian national) received a five-year prison sentence for spy activities performed on behalf of Russia’s GRU (military intelligence). In 2016, three suspected Russian spies were jailed for “activities against the state.”

Since leaving the Soviet Union, several high profile spy cases involving NATO-linked



Head of ISS Arnold Sinisalu

operations have occurred in Estonia. Russia still has the backing of thousands of Estonian citizens.

Moscow refused to comment on the Vasilyev case, but the Russian Ambassador to Estonia, Alexander Petrov, said: “The man is 20-years-old.

We don’t understand why this theory was voiced.” He went on to say that the move was probably made to “generate public opinion” [against Russia].

2017. NATO Deputy Secretary General Rose Gottemoeller with British troops in Estonia



SRI Director Eduard Raul Hellvig

UNITED KINGDOM EYES ONLY



MI5 headquarters, London

TERRORISM AND HORIZON THREATS

Theresa May Assassination Plot Foiled

As MI5 Director-General Andrew Parker spoke about the threat to the UK from ISIS and again referenced the foiling of nine significant terrorist plots in 2017, two men arrested on 28 November, appeared in court charged with terrorist offences, including a plan to assassinate UK Prime Minister Theresa May. Details of the plot were disclosed by Mr Parker in a briefing to Cabinet officials, but details soon began to trickle into the wider media.

Naa'imur Zakariyah Rahman, 20, from London and Mohammed Aqib Imran, 21, from Birmingham, were arrested in a joint operation by counter-terrorism officers and MI5.

The alleged plot, which some security specialists believe was ill-conceived, was for Rahman to blow up the gates protecting Downing Street using an improvised explosive



The suspects
are driven into
court

device (IED) hidden inside a bag. Then Rahman would use pepper spray to force his way inside Number 10 while wearing a suicide vest, and kill May with a knife.

When officers from CTC (New Scotland Yard Counter Terrorism Command) searched Rahman's home, he reportedly had two IEDs on his person. He is also accused of assisting Imran, who MI5 believe was planning to join ISIS by obtaining a fake passport in the hopes of reaching Libya.

MI5 ANALYSIS

This latest court case linked to terrorism involving ISIS supporters, coincides with an independent review of MI5's own internal investigative probe* examining if any of the significant UK terror attacks to have taken place in Britain in 2017, could have been prevented. In his publicly available 66-page



MI5 Director-General
Andrew Parker



David Anderson QC

report, David Anderson QC (Queen's Council), a former terrorism law reviewer, noted references to analysis; there were also several 'if's' regarding

procedures, but in general, mild criticism was removed by the word hindsight. For example, it was 'conceivable Manchester Arena bomber Salman Abedi could have been stopped' performing the May 2017 attack which killed 22 people. Anderson highlighted the fact that

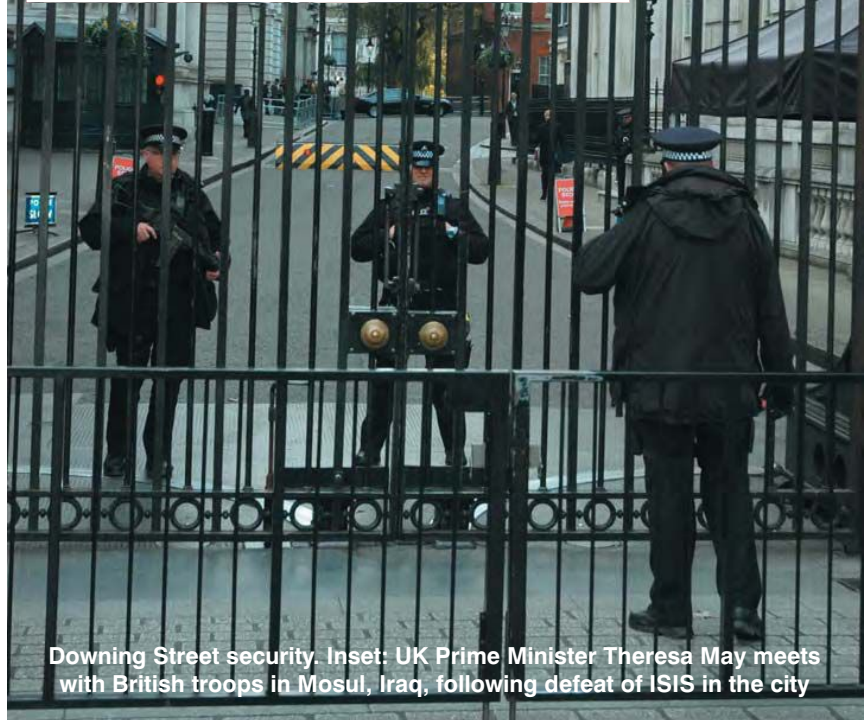


Salman Abedi

Abedi, designated SOI (Subject of Interest) had previously been under surveillance and his case was to be reassessed. Had surveillance been reinstated and approved sooner, his plot may well have

been exposed. It was not - MI5 mistook him for someone else and the case was closed.

The theme of surveillance, hindsight, analysis and procedures was projected several times,



Downing Street security. Inset: UK Prime Minister Theresa May meets with British troops in Mosul, Iraq, following defeat of ISIS in the city

and especially focussed on events between March and June when a combined total of 36 people were killed and over 300 injured in various attacks. However, MI5 recently disclosed that 20,000 people are being monitored with a further 3,000 registered as

SUBJECTS OF INTEREST (SOI) MI5 PRIORITISATION SYSTEM

PRIORITY 1: Investigations into individuals or networks where there is "credible and actionable intelligence" of significant or smaller scale attack planning

PRIORITY 2: Investigations relating to individuals involved in travel overseas to join Jihad, fundraising, training and supply of false documents

PRIORITY 3: Investigations or networks that require further action to determine whether they pose a threat

PRIORITY 4: Those who had once posed a serious threat where there is a risk they may re-engage in extremist activity

CLOSED SOIS: The 20,000 closed cases of people no longer actively subject to investigation



Flowers and tributes for victims of the Manchester attack



Joint UK Police/Ministry of Defence unit outside a London building



UK CTC Police and a British soldier at the gates of Downing Street

'elevated targets'. Ultimately Mr Anderson said there was no real knowing if the Manchester plot could have been prevented if MI5 had acted differently. However, he did say: "With the benefit of hindsight, intelligence was misinterpreted in early 2017."

DEAD TERRORISTS POSE NO THREAT

UK Defence Minister Gavin Williamson has spoken out on the threat posed by returning UK nationals who have fled ISIS fighting forces in the Middle East. He said not a "single British citizen who has fought for Islamic State should be allowed back in Britain." He believes that a number of initiatives being discussed - resettlement of an estimated 300 UK nationals who may attempt



Max Hill QC

threat." His comments follow a suggestion made by Max Hill QC, Independent Reviewer of Terrorism Legislation that some young ISIS people who travelled to the fighting zones be allowed to return and rejoin society. His focus was on those who had been brainwashed and could be categorised "immature and vulnerable teenagers." Other comments he said

to return to the country - are flawed. Williamson said: "Quite simply, my view is a dead terrorist can't cause any harm to Britain. We should do everything we can to destroy and eliminate that [the]

were misrepresented in some quarters. His full response can be found on the Independent Reviewer of Terrorism Legislation website.

RECORD NUMBER OF ARRESTS

In the year ending September 2017, Britain's security services arrested a record 400 people on terrorism-related offences. Of these, 115 were charged, 60 were released on bail pending further investigation, and 11 faced alternative charges. Interestingly, intelligence sources said 58 were female. Security Minister Ben Wallace said the figures reflect the menace of terrorism and show a "shift" rather than a "spike in terror arrests." MI5 D-G Parker said the scale of terrorism is evolving as never before: "Today, there is



UK Secretary of Defence Gavin William and USA Defense Secretary James Mattis meet to discuss homeland security



Armed police in Manchester



A British soldier inside the perimeter of Downing Street



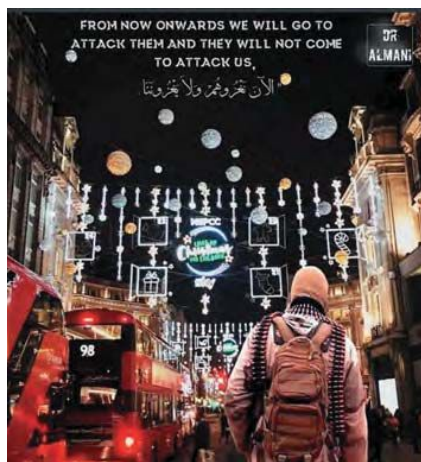
Ben Wallace

more terrorist activity coming at us more quickly and it can be harder to detect."

*Original investigative review runs to 1,000 pages.

'CHRISTMAS IN OXFORD STREET'

ISIS released a series of posters threatening attacks during the Christmas festive period in major cities, including London, New York and Paris. One shows Santa Claus standing in Times Square next to a box of dynamite.



MI5 COUNTERMEASURES AND RESPONSES

In June 2017, following several terrorist attacks, MI5 and Police officials commissioned an internal review and an Operational Improvement Review (OIR)

MI5 STATEMENT: David Anderson QC's report endorses several recommendations that MI5 and Police believe will further strengthen processes in counter terrorism work. Many of these build upon existing improvements already underway at the time of the attacks. The main areas of focus are:

• **EXPLOITING DATA:** the OIR recommends steps to strengthen further our ability to detect engagement in terrorism-related activities, including detecting re-engagement by former subjects of interest in terrorism investigations.

• **MULTI-AGENCY ENGAGEMENT:** the OIR recommends going beyond existing relationships to enable the widest range of partners to be engaged in managing the risk of renewed engagement in terrorist-related activity as part of a whole of Government counter terrorism response. This includes specifically a new commitment by MI5 to allow knowledge



derived from intelligence to be shared more widely beyond intelligence circles.

• **INCREASED ROLE FOR THE JOINT TERRORISM ANALYSIS CENTRE (JTAC) AND MI5 IN DOMESTIC EXTREMISM:** the OIR proposes to bring equivalence of processes between the current approach to domestic extremist threats (such as right wing threats) and Islamist terrorism, by strengthening threat assessment processes and joint working between CT policing and MI5 where there are potential terrorist threats in this area.



MI5 headquarters



Finally, the OIR recommends a number of technical changes to improve existing operational counter terrorism processes. These cover processes such as information management and the handling of intelligence.



**Eye Spy Editorial concludes
its journey examining
the changing dynamics of
communications spycraft**

NOTES: COMMUNICATION & ESPIONAGE

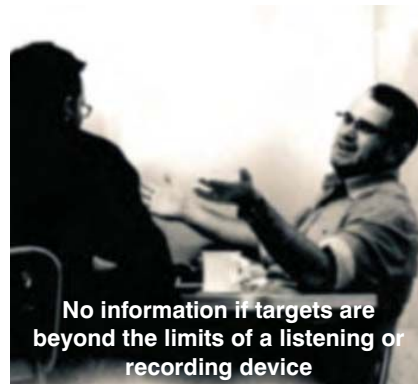
ADVENTURE IN TIME

There was a time, not too long ago, many leading intelligence academics predicted the 'spy-in-the-sky' satellite and advances in the interception of electronic signals and messages, would put pay to the activities of the human spy on the ground. On the contrary, quite the opposite has happened, and those who operate in today's world of intelligence have even more reason to celebrate and trust the tradecraft of their predecessors. For as one former MI5 agent told Eye Spy, "despite CCTV, 24-hour sky surveillance and tools to intercept e-mails and telephone calls, spycatchers and counter-terrorism chiefs often struggle to see the bigger picture... and you still can't intercept and record a conversation if the participants are beyond a microphone."

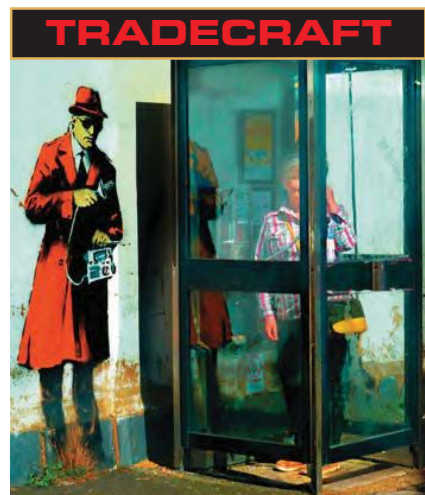
VISUAL, AUDIBLE, TOUCH

No matter how many methods can be used to pass information to a third party, it can only be absorbed three ways: by sight, sound, and in some cases by touch. Yet it is all that has gone on before that interests so many

'connoisseurs of espionage', and this often means overcoming hurdles, each one capable of tripping spies and the recipient of secrets. To guarantee maximum security, intelligence agencies will use all manner of 'cloak and dagger' to conceal activities, from couriers and cleverly written features or notices in the world's press, to the passing of instructions or notices contained within radio broadcasts. And for a good example of the use of radio as a very strong and secure method - look no further than the UK's very own British Broadcasting Corporation (BBC).



**No information if targets are
beyond the limits of a listening or
recording device**



THE DICE ARE ON THE TABLE

Throughout much of WWII, the BBC broadcast all manner of secret messages across Europe, and in particular France. Designed specifically for a chosen few, some broadcasts carefully concealed (unrecognisable) lines prepared by military intelligence specialists and agent



1944. Resistance fighters in Boulogne - radio was their lifeline

controllers. To the layperson, these were no more than 'jargon' - puzzling phrases and what most would describe today, as strange. Not that these transmissions, usually relayed in French shortly after a few minutes of news, completely fooled the listeners of the German High Command in Berlin. After the news, a broadcaster would announce: "Et voici quelques messages personnel" (And here are a few personal messages).

Examples in historical military books are numerous, but make of these what you will: *'Andromache scented with lavender'*; *'Anthalie remained in ecstasy'*; *'I love Siamese cats'*; *'Clementine can pick his teeth'*; *'There is a fire at the insurance agency'*; *'The dice are on the table'*. The very last one in fact, was an SOE command to the Free French Resistance to start attacking and disabling trains and railway track.

In reality, they are *all* covert instructions to Resistance cells, sometimes encased or mixed with meaningless phrases. To the waiting recipients of a specific line, once delivered they often advised the location of a supply drop, or where an Allied agent would be entering or exiting the country. Occasionally, they were a 'green light' to signal the beginning of an operation, as in the case of *The dice are on the table'*. Many were unique to specific cells or individuals controlling or operating in occupied regions. Whilst the Germans recognised the importance of the material they were intercepting, its value was worthless unless understood. And just like intercepted messages today, this frustrating factor remains a constant... if data can't be interpreted or understood, the intelligence is worthless, save its evidential use to connect parties.

As history shows, German Intelligence eventually detained SOE agents in Europe, who under interrogation, provided intimate details and sometimes meaning to the BBC radio broadcasts. At least the Abwehr now had confirmation radio was being used to direct and instruct covert anti-Nazi forces. And there are case files, in Holland for example, which show Allied operations were exposed and many operatives captured and executed.

THE CODEMAKER

In 2001, following 9/11, MI6 working with colleagues in the CIA, discovered an elaborate al-Qaida operation directed by Osama bin-Laden, that was evidence enough the terror



Mohammed Khan

group's command structure and influence went far beyond simple 'attack stratagem'. A 'book', dubbed the Al-Qaida Alphabet (a document - both printed and virtual), was discovered containing translations and word replacements using code to reference hundreds of locations, targets and 'helpers'. For example, the World Trade Center



1941. French leader in exile, Charles de Gaulle speaks to his countrymen from BBC radio studios in London. The broadcaster was used extensively by the SOE, MI6 and War Office to relate covert communications to Resistant fighters and agents across Europe



was codenamed the 'faculty of town planning', Capitol Hill, the 'faculty of law' and the Pentagon, the 'faculty of fine arts'.

It was designed to defeat listening NSA and GCHQ programmes which AQ feared could 'grab' such terms from the airwaves, through telephone lines or Internet (e-mail) exchanges. It probably stems from conversations bin-Laden had prior to 9/11, which for reasons still unknown, managed to find their way into the press. Such was bin-Laden's fear of exposure, he hired couriers to travel and deliver alterations in the codebook's alphabet, thus adding further layers of security. One man who was pivotal to the creation of the covert alphabet was Mohammed Naem Noor Khan, aged 25 in 2004 - the year of his downfall.



Lahore International Airport - now Allama Iqbal. Inset: Crest of the ISI



The former Metropole Hotel, London. MI9 was originally based here

Red cross parcel intended for POWs and OSS silk escape map and compass. Numerous such items were secreted to prison camps by Britain's MI9

Known to MI6 as the 'codemaker', the university graduate used a constant 'rolling alphabet' that was only known to his trusted inner circle, and those engaged in operations.

His capture stemmed more from good fortune than detection. The ISI had discovered a cell phone attached to an IED intended to explode on a roadside in Karache. The CIA joined the investigation and after careful examination of the cell phone an address was discovered. Here Pakistan Inter Services Intelligence Agency (ISI) officers arrested Mussad Aruchi, the nephew of a known AQ agent. He talked and identified Khan as an "agent controller." Located and placed under surveillance, Khan was arrested at Lahore International Airport on 13 July 2004, by the ISI. He had driven to the airport to collect a package. At associated addresses laptop computers and 50 CD-Roms were discovered containing full details and a comprehensive listing of the so-called Al-Qaida Alphabet.

TIME NO BARRIER TO INTELLIGENCE

The understanding of communications, no matter how simple or complex, is therefore crucial to counter-intelligence, and the operations masterminded by the likes of Khan and the SOE in wartime London, are evidence enough that any breach can be enough to penetrate and disable covert activities, be they for the good or otherwise. For the record, AQ operatives use of word exchange continued for the next decade, but now alerted, international security services were more watchful. MI5, for example, is just one organisation that

successfully investigated and derailed several terrorist operations where cell members chose to conceal plots using language of hidden meaning.

Many examples of this tradecraft exist, perhaps one of the most famous being the operation run by MI9 in WWII. Here captured British troops sent letters back home to loved ones... who duly deposited them with MI9 in London. For the communications contained hidden messages about German military strengths, positions and armaments. In return,

letters would be written back also containing secret instructions and messages. Occasionally secreted in food parcels, MI9 managed to conceal maps and guidance on where best to exit Germany in respect of escape routes.

MARATHONS AND FLAGS

Communication is an art thousands of years old. And adaptations of some historical methods continue to this day. In Ancient Greece, troops would communicate using fire (beacons) at the top of hills and mountains.



A painting by Luc-Olivier Merson (1869) depicting the moment Phidippides informed Athens of the defeat of the Persian Army - and a possible counter-attack



US Navy sailors using flag semaphore



This speedy method allowed armies time to be assembled and villages to be readied for evacuation in the event of invasion. One communication event involving the Greeks will be forever etched in the history of Mankind and spylore. In 490BC the Greeks defeated the Persians in the Battle of Marathon. Fearful that the retreating Persian army would make their way to Athens and attack the city, its military commander gave a man called Phidippides a message to take back to the city. Contained within, news of the victory, but a warning to prepare for possible action. Phidippides ran

the 26 miles distance in around three hours giving Athens valuable time to prepare. Sadly for the 'Marathon runner', he died from exhaustion. And of course today, the Marathon race is recognised and run throughout the world (long distance).

For the record, it was also the Ancient Greeks who first utilised the 'services' of pigeons as couriers. Enough has been recorded about their involvement as a rapid communication device in espionage and military matters! And the origins of 'flag signalling' is also thought to have originated in Greece (450BC). This of course evolved over the years, and many navies opted to utilise flags to send coded messages, instructions and general information, especially in time of conflict or as a warning notice. Today, maritime flag signalling (semaphore) has evolved into the International Code of Signals (ICS).

fighting forces, as it was to the Greeks two thousand years earlier.

SIGNALS, DRUMS AND SMOKE

In the 1700s, the French used a signalling system also called Semaphore to pass information great distances. In this case Abbot Claude Chappe invented an early signalling



Above: Painting of an original Chappe Semaphore station. Below: Illustration of a coastal station using the communications and code system in coastal waters



The Romans established a communication network allowing horseman to convey messages upto 300 miles a day

RUNNERS AND RELAYS

The Roman Army also utilised runners to convey messages. As the Roman Empire expanded, it was necessary to embark upon the creation of a courier network. In this case they created the Cursus Publicus or State Runners Service to navigate and speedily cross huge expanses of countryside. At outposts around eight or nine miles apart, riders could exchange tired horses to continue their journey uninterrupted. Occasionally, remarkable distances of 300 miles a day were achieved. The word relay was used, and like events at Marathon, this too evolved into an Olympic event.

Another country which utilised runners and relays to deliver messages was China. This was first recorded in the 13th century by a visiting Marco Polo, who also noticed the participants used bells on their clothing to alert the next runner of his approach. And in the Great War of 1914-1918, the use of runners on the battlefields of Europe to convey messages was as important to the respective



Abbot Claude Chappe

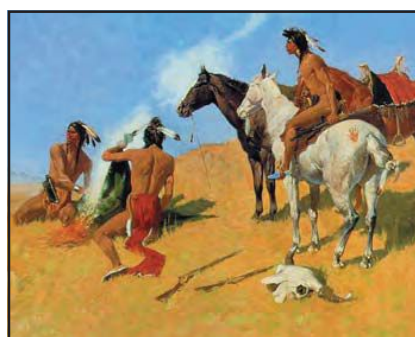
system that used a very tall post in which wooden arms could be moved to represent letters. Stations were situated on hill tops sometimes many miles apart, but the distance was overcome by using telescopes to note the moving arms. In later years, Semaphore was also used to communicate with ships at sea from coastline stations. Historians claim the system, sometimes referred to as 'Claude's Telegraph', was so successful, a message could be 'transmitted' 80 miles in just a few minutes by experienced operators.

Besides the soldiers of Greece using fire to communicate, Native Americans also utilised this earthly element, in this case limiting or increasing smoke plumes. Rings of smoke often contained hidden messages, warning of danger or announcing the safe return of a hunting party. The use of smoke as a signal, especially as an emergency marker and/or battlefield prompt continues to this day.

Similarly, the use of audio as a form of signal can be traced back hundreds of years. Native



**Main: Coastal Chappe Semaphore (telegraph) station in France.
Inset: A replica built in Nalbach, Germany**



**Native Americans send a smoke signal.
Below: Coloured flare as signal**



Americans (and other peoples) used certain drum beats and armies throughout history have used audible arrangements to start a specific action.

MOVING INTO A NEW WORLD

In WWII, the British public were advised to be "watchful for enemy spies," and there are numerous case files which reflect a nervousness sweeping the country. One women's story of a suspicious neighbour even reached the codebreakers of Bletchley Park. She reported a person who she believed was communicating in Morse code. The reason? Her neighbour was hanging out her washing in a particular fashion... one short garment next to a long one and so on. However, there are cases in spylore that seem to confirm some agents did in fact use *specific* clothing placed on washing lines on *specific* days to relate messages! Another covert method was to hang coats and jackets with certain buttons missing or replaced by similar, but not identical ones. All had a meaning to the recipient (observer).

Long before instant electronic communication, numerous odd methods of passing or receiving messages covertly existed, from utilising curtains, in this case widening or lengthening the gap between the curtains, to placing flowers in windows, switching the colour of lightbulbs, or even leaving a matchbox on a pub table with matches



Clothes and buttons - used as secret signals



Matches - once upon a time used by spies



Besides normal use, airport running lights can be utilised to communicate with aircraft

deliberately cut to certain lengths. All had a meaning to the observer or recipient.

The KGB used drawings and chalk to convey messages and various case files exist reflecting this 'art'. One former MI5 operative told Eye Spy how, in conversation with contacts in pubs, he used to leave a calculated number of cigarette filters (butts) in an ashtray to signify how much he was prepared to pay for information. Of course in all cases, the end user must also be familiar with what each event or object actually represented. Spy trade is limited only by the imagination of each user, and often simple tactics are far more beneficial, and in most cases, safer and secure. Word of mouth is a good example, though this by necessity means the engagement of two parties.

To offset danger of exposure, there are numerous ways in which agent contact can and is made, and there are several tradecraft features which have appeared in Eye Spy covering this topic. But some are considered safer than others. A busy location, or alternatively, one that is remote and away from people, in a spacious park for example. When extra levels of security are required, (usually an indication of the quality or importance of intelligence to be imparted), then preparation of contact is inevitably arranged and elevated to those whose experience in this tradecraft element is recognised.

INFORMATION OASIS

MI5 Director-General Andrew Parker, a counter-terrorism specialist, believes there should be nowhere on the Internet where those intent on terrorism and underworld activities should be able to communicate, safe in the knowledge that they are protected by a 'digital oasis'. And this was one reason (amongst many), why the actions of NSA contractor Edward Snowden, so incensed US Intelligence.



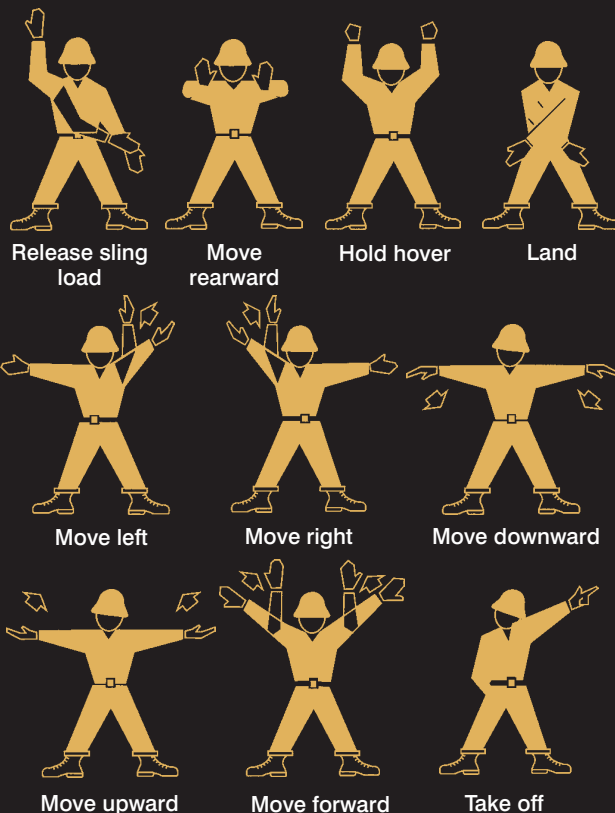
MI5
Director-General
Andrew
Parker

The thousands of documents Snowden released into the public domain, reveal so many [NSA and GCHQ] communication and interception 'secrets of the trade'. This has allowed "full sight of agency tracking secrets," according to Stephen Phipson, of the UK Office for Security and Counter Terrorism (OSCT). Indeed, once the material began appearing, known terrorists, supporters and sympathisers, began changing the way they related messages. Andrew Parker said the leaks had caused "enormous damage and given terrorists a gift to be able to attack Britain at will."

Continued on page 80



HELICOPTER HAND MARSHALLING SIGNALS



US Code of Federal Regulations. (Other variants exist)

INTELLIGENCE NOTES

JERUSALEM

US Recognises Jerusalem as Israel's Capital

Opening Pandora's Box?

On 6 December 2017, President Trump declared that the United States recognised Jerusalem as the official capital of Israel, though added a caveat: "We are not taking a position of any final status issues." He also said the US Embassy would be relocated to the city, though no time-frame was given. It was a decision welcomed in Israel, but with dismay by many nations and the Palestinian people themselves. Security and intelligence figures said tensions would rise and probably lead to more conflict. Demonstrations and outbreaks of violence did erupt outside a number of US embassies.

The status of Jerusalem, one of the most sacred religious sites in the world, has been disputed for years. Both Israelis and Palestin-

ians claim the city as their own, and as such, a status quo has operated running parallel and inextricably linked to talks about a lasting peace deal. The United Nations, Europe and many Arab nations believe that such an agreement must be in place before final talks on the city's future begin.

Since the 1948 Arab-Israeli war, when Israel seized approximately 50 per cent of the city, the UN regarded it (and surrounding areas) a 'special international zone'. Within the offices of the UN and many an intelligence headquarters, it was hoped that a peace deal would lead to western Jerusalem being governed by Israel, and the eastern sector by a future Palestinian state. President Trump's announcement has effectively circumnavigated all earlier and current processes and broke



Israeli troops in Jerusalem

with traditional neutrality, though he still wants both parties to talk peace.

Israel's Prime Minister Benjamin Netanyahu called for other nations to follow Washington's lead, but at time of publication, no European

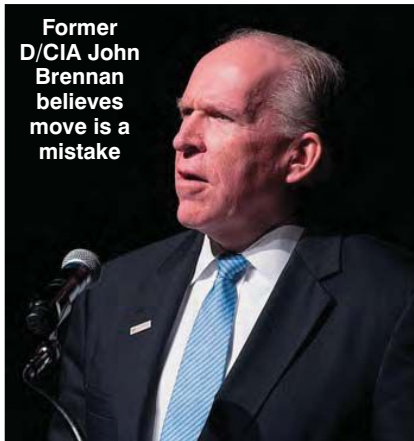


US Embassy, Tel Aviv



July 2017. Israel's Prime Minister Benjamin Netanyahu with Admiral Michelle Howard, Commander Naval Forces Europe, aboard the USS George H.W. Bush. Netanyahu welcomed the decision to recognise Jerusalem as Israel's capital

Former D/CIA John Brennan believes move is a mistake



nation has done so. Various countries, including Australia, Canada, Denmark, Mexico and Italy, to name but a few, said they would continue to operate their respective embassies from Tel Aviv.

In keeping with current policy, France, and even the Czech Republic, one of Israel's closest allies, said the status of the city could only be resolved when a permanent peace deal is agreed. Turkey President Recep Tayyip Erdogan said the announcement represented a "red line for Muslims," a move which could derail renewed relations with Israel following a six-year hiatus. World leaders generally accept that a two-state solution is the correct approach.

INTELLIGENCE PERSPECTIVE

As for the majority of intelligence people, including those within the US intelligence community (USIC), most believe America has just abdicated its long role as an authentic arbitrator in the peace process.

Michael Hayden, former Director of the CIA and NSA said: "I think there is a reason - a good reason that previous president's have

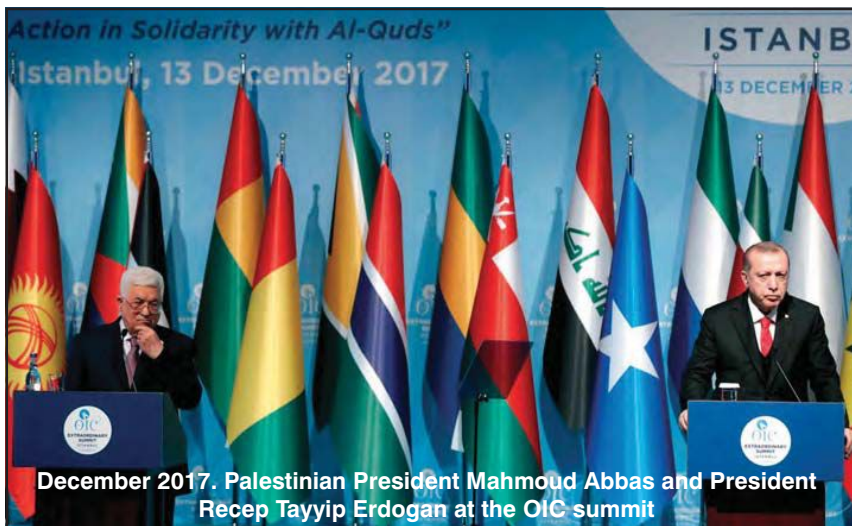


avoided taking that step (with Jerusalem)... the detail in what Trump said matters." He also called the relocation of the US Embassy to Jerusalem, "a dramatic move." This vastly



In response to President Trump's announcement, leaders and officials of the 57 Muslim majority nations'

OIC (Organisation of Islamic Cooperation), gathered for an emergency meeting in Istanbul. The summit was called by Turkish President Recep Tayyip Erdogan, who declared: "I am inviting the countries who value international law and fairness to recognise Jerusalem as the capital of Palestine."



It wasn't just Muslims who protested the Jerusalem decision. Archbishop Pierbattista (right) and 12 senior Christian leaders in the city sent a letter of protest to the US President, saying it would lead to even deeper divisions





Just three hours after President Trump's statement, Britain's Foreign Office gave this advice on travel to Jerusalem: *'Following President Trump's announcement recognising Jerusalem as Israel's capital on 6 December, Palestinian factions have called for mass protests across the West Bank, including East Jerusalem, on 7 and 8 December; the security situation could quickly deteriorate, particularly around the Old City of Jerusalem; you should avoid all demonstrations across the West Bank and follow the advice of local police authorities'.*



HRH Prince Turki al-Faisal

work with a "new mediator to create a two-state solution."

If the US does relocate its embassy from Tel Aviv to Jerusalem, sources believe it will not be fully operational until 2022. The United States, like many other countries, also operates a consulate from Jerusalem.

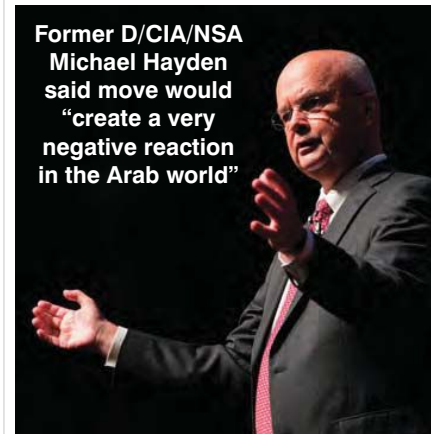
experienced intelligence man believes it is connected to a US Government signal issued just days earlier, that warned American embassies and consulates of potential trouble. "It's going to create a very negative reaction in the Arab world," he said.

Another CIA man, former Director John Brennan called the decision a "reckless and foreign policy blunder of historic proportion." He warned the announcement "will damage US interests in the Middle East for years to come and make the region more volatile."

His words were echoed by former Saudi Arabian GID intelligence head (Al Mukhabarat Al A'amah) and Ambassador to the United

States HRH Prince Turki al-Faisal. "The move is a domestic political ploy and would stoke violence," he said.

Palestinian President Mahmoud Abbas said Trump's decision violated international law. "The US can no longer function as a diplomatic sponsor and peace mediator," he said. Mr Abbas met President Trump in May 2017, and insiders say there was no reference or indication Mr Trump was to recognise Jerusalem as Israel's capital. Palestinian Foreign Minister Riad Malki said the US has "withdrawn from the peace process and positioned itself as an actor." He did say his leadership had "no intention of withdrawing from peace negotiations," but would look to



Former D/CIA/NSA Michael Hayden said move would "create a very negative reaction in the Arab world"

THE SUBWAY BOMBER

Attempted-ISIS Inspired Terrorist Attack in New York

On 12 December, Bangladeshi national Akayed Ullah, 27, detonated a pipe bomb, attached to his person with velcro and zip ties. The explosion occurred in a busy subway station walkway at New York's Port Authority at 7.20am - when thousands of city residents were making their way to work. Four people suffered injuries but Ullah, who suffered extensive burns, survived. Within two hours, Mayor Bill de Blasio and security

officials confirmed the incident was one of terrorism.

The lone wolf terrorist moved to the USA in 2011 and lived in Brooklyn where he worked as a taxi driver and electrician. He sourced instructions for the IED from the terror magazine *Inspire*. The crude device was made from hundreds of matchstick heads, a sugar composite and fairy lights.

The location chosen by Ullah links the Port Authority Bus Terminal to Times Square and is one of the busiest in the world - serving about 225,000 commuters a day. It is considered a 'soft target' by police officials because it does not have the same security as an airport.

ANALYSIS

Of relevance, the failed attack came just days after the 'Muslim Day of Rage' protests in Dhaka, Bangladesh's capital, where thousands



of people had gathered to vent their disapproval over President Trump's declaration recognising Jerusalem as Israel's capital. Ullah told detectives his actions were in response to the Jerusalem announcement, events in Gaza, and attacks against ISIS. "I have been following ISIS on the Internet," he allegedly said, "I did it for them." Former NYPD Commissioner Bill Bratton confirmed that the suspect "supposedly set the device off in the name of ISIS." Also of note, investigators discovered a message Ullah had posted just hours before the attack - *'Trump you failed to protect your nation'*.





Various raids ensued following Ullah's attack

There was much speculation in the media that Ullah was heading towards a target in Times Square itself, and that the device had exploded prematurely. Investigative officers from NYPD's Joint Terrorism Task Force and the FBI rejected this scenario after Ullah told them he deliberately chose his location because it was full of Christmas decorations and advertising. "Ullah was aware of previous ISIS attacks at Christmas markets in Europe, and he knew exactly where he wanted to detonate his bomb," a police source told Eye Spy associates in the city.

Raids ensued at addresses attached to Ullah and a number of people were taken away for questioning. In faraway Bangladesh, the country's counter-terrorism service questioned Ullah's wife and a number of relatives.

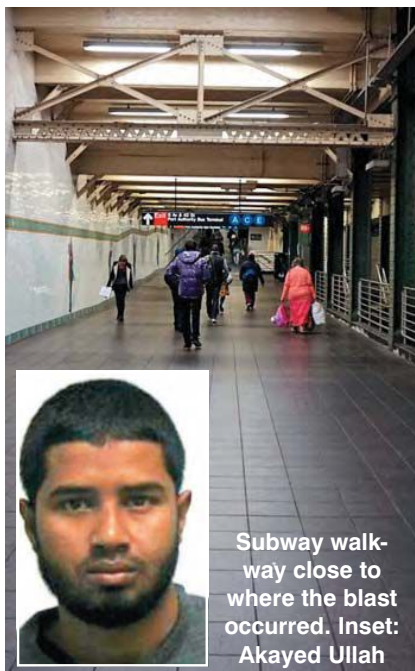
New York Governor Andrew Cuomo said a "bombing in the Subway is one of our worst nightmares... but New Yorkers will get through



Akayed Ullah is taken to hospital

this as they have before on 9/11 and the recent terror attack on Halloween. We have the Statue of Liberty and that makes us an international target." He also acknowledged that anyone can use the Internet to download instructions on how to make bombs. "That is the reality we have to live with today," he said.

President Trump blamed lax immigration policies and again urged Congress to "enact legislative reforms to protect the American people."



Subway walkway close to where the blast occurred. Inset: Akayed Ullah



New York Port Authority officers Sean Gallagher, Drew Preston, Jack Collins and Anthony Manfredini attended the bomb scene immediately and detained Ullah

SPECIAL REPORT

DARK WEB



Cyber Specialist and Eye Spy
Associate Editor

KEVIN COLEMAN provides
an insight into one of the
most important and little
understood subjects facing
those working in cyberspace
- the DarkWeb

Espionage and all manner of covert activities, many illegal, exist and thrive in the expansiveness of the DarkWeb. A large number of users of the Internet have not even heard of the DarkWeb, whilst those that have, may not fully understand this deep, dark connected world.

DarkWeb is a massive area that remains a great mystery and challenge for security services and the intelligence community; a huge portion is clandestine and lies hidden in cloaked networks of the World Wide Web. It is also referred to (rightly and wrongly) as Darknets, Hidden Web, Deep Web, Deep Net, Invisible Web, and Undernet that use the Internet for connection and communications. Each requires specific (highly guarded and restricted) software, encryption, as well as special authorisation and configurations for access. Basically, this includes all the websites and systems that are connected to the Internet that are not readily visible to you and me, available or known, or indexed by recognised search engines.

INTEL: The DarkWeb has its own Wikipedia-like site to assist those trying to navigate its shadowy world.

Specialists participated in a study to estimate the size of the DarkWeb; resultant analysis suggests that it is about 4% of the total Internet. It should be noted that not everyone accepts this figure. Another circulated figure contends that the DarkWeb is about 500 times the size of the known Internet indexed by search engines. Researchers speculate the size of the DarkWeb approximates 7.5 petabytes - this represents a very large amount of information.



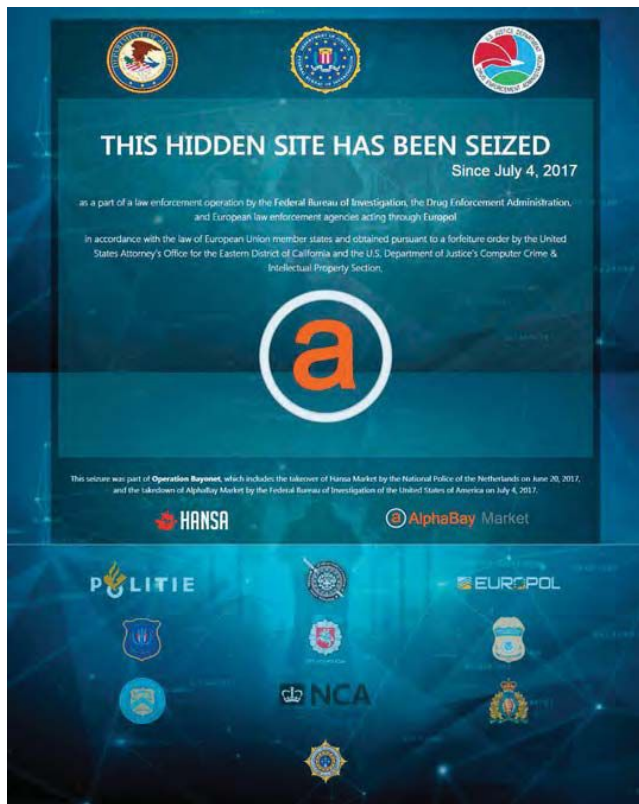
Since these studies were published, the DarkWeb has likely grown (some say significantly). There is no accurate accounting for the DarkWeb and even less information about the value of the commerce that occurs in it; in truth, no one knows how big the DarkWeb actually is or how fast it grows.

Some specialists have predicted the demise and the eventual collapse of the DarkWeb. Others say it will continue to evolve. "Those who talk of the downfall of the DarkWeb clearly do not understand the magnitude of this revolution," a senior source said.

ACCESS

INTEL: The first step in accessing the DarkWeb is thought to be installing and using the TOR browser - [www.torproject.org]. It should be noted that not all DarkWeb sites use the Tor Browser tool, whilst other sites require specific configuration. There are also unconfirmed reports that some sites actually require special hardware. Those who engage this area of the Internet can purchase just about anything with a few mouse clicks. The DarkWeb is the premiere global marketplace for the sale and purchase of illegal goods, products and services.

An Intelligence Perspective



Those attempting to enter the DarkWeb sites of AlphaBay and Hansa were greeted with this notice



FBI graphic identifying the number of users on AlphaBay and the type of services provided

Now let's take a look at five of the most problematic issues confronting the intelligence and security world that are found on the DarkWeb.

CYBER ESPIONAGE & RELATED ACTIVITIES

In terms of hacking, you can anonymously purchase (hire) the services of a hacker to spy/track a person, conduct cyber espionage, place illegal content on a computer and tip-off

the police, plus so much more. While it has been the prime source for cyber weapons and exploitation kits, it has branched out significantly. All these 'services' are payable via a cryptocurrency.

STOLEN INTELLIGENCE AND INFORMATION

The DarkWeb has been used by whistleblowers who acquire classified information (some top secret) and usually put



FBI Acting Director Andrew McCabe, flanked by Attorney General Jeff Sessions (right) and Deputy Attorney General Rod Rosenstein discuss the closure of AlphaBay, the largest DarkWeb marketplace in the world



All major cyber intelligence agencies now monitor the DarkWeb

it up for sale or hold it for ransom. There are also reports that some major media players (news desks) actually have a DarkWeb web address (URL). A so-called 'strong box' is located there that allows individuals to upload documents without the fear of being tracked and identified.

POLITICAL INFLUENCE

The DarkWeb's obscurity and anonymity has made it an excellent avenue through which to source and initiate political attacks. It has been described as a "hot resource for hackers" carrying out their illegal tradecraft and offering "tools for political attacks."

Sources have also reported the DarkWeb is a premier source for voter registration data fraud. The price varies for services provided, and of course, all require cryptocurrency as payment. ➤



ELECTRONIC WEAPONS

An example of a recent sale was a cigarette pack-size device, said to be an electromagnetic pulse (EMP) weapon. The price listed was around \$2,000 payable with a cryptocurrency. Generally speaking, an EMP device destroys electronics like computers, cell phones, industrial controls, new vehicles, radios and much more. This device is effective if the electronics are in very close proximity (estimated at a few feet).

ILLEGAL DRUGS

The anonymous DarkWeb sales of opioids and other illegal drugs are booming and unfortunately people are dying. The prevalence of



Alexandre Cazes - founder of DarkWeb site AlphaBay

illegal drugs ordered over the DarkWeb is anything but small. It's no secret that law enforcement has become increasingly frustrated about growing sales of narcotics on the DarkWeb and the use of cryptocurrencies for payment.

INTEL: DarkWeb sites exist with highly encrypted digital rooms that facilitate secure multi-mode communications live audio/video and graphic (PowerPoint Slides).

IMPLICATIONS

The DarkWeb coupled with cryptocurrencies work together to make a seemingly unbeatable combination. Cryptocurrencies was referenced in my report (See Eye Spy 111)



US Government security specialists attend a cyber conference

NO HIDING PLACE NCA

Following the closure of AlphaBay and Hansa, Ian Cruyton, Deputy Director of the NCA, said: "Two of the most significant DarkWeb criminal marketplaces are now permanently offline, seriously affecting the capability of several criminal networks. Law enforcement agencies will now begin to sift through the forensic material gathered during the strikes. The criminals who used these sites would be right to fear the outcome of those investigations."

"The DarkWeb may appear to offer criminals a degree of anonymity but law enforcement agencies are able to exploit that cover themselves and have a whole range of tools to go after their targets."



addressing the general use of new forms of money. One can only imagine that the high degree of anonymity associated with cryptocurrencies (some more than others) is at least partly responsible for the dramatic growth in espionage, clandestine operations, criminal activity and the sale of stolen or otherwise ill-gotten information.

PRODUCTS AND SERVICES

Payment for information, espionage and clandestine operations: There are no accurate or definitive figures for the monetary value of the sale of stolen or otherwise illegally acquired information (logins, passwords, credit card numbers, birth dates, social





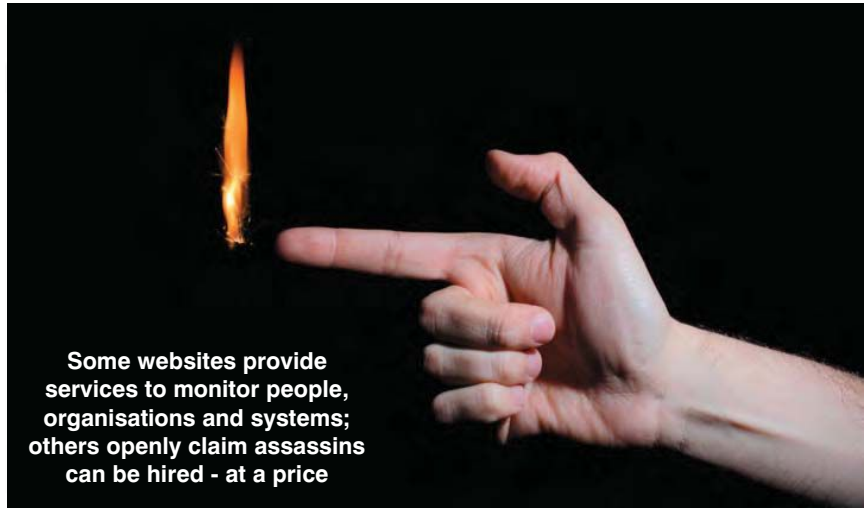
Firearms can be found for sale on the DarkWeb

security numbers etc.), espionage activities or clandestine operations. However, there are estimates, and one analyst placed its value in excess of \$220 billion and growing fast.

Payment for the illegal sale of weapons: An accurate figure for the global value of the illegal international sales of conventional weapons has never been possible. The best estimates at this point indicate the illegal small arms trade exceeds \$100 billion. The human costs are far greater.

Payment for the illegal sale of cyber weapons: There is a large and growing global market for the sale of cyber weapons and the components that make them possible (Zero-Day vulnerabilities). The current DarkWeb/Black Market price for a cyber weapon designed for a popular smartphone is over \$250,000.

Payment for illegal and clandestine services: There is at least one DarkWeb site that lists the services of individuals and organisations willing to engage in assassination. One stated they will even provide photos as proof that the 'job' has been done. Another payment service allows monies (mostly cryptocurrencies which can be compared to a pay check in this case) to be transferred to those employed by some of these criminal organisations.

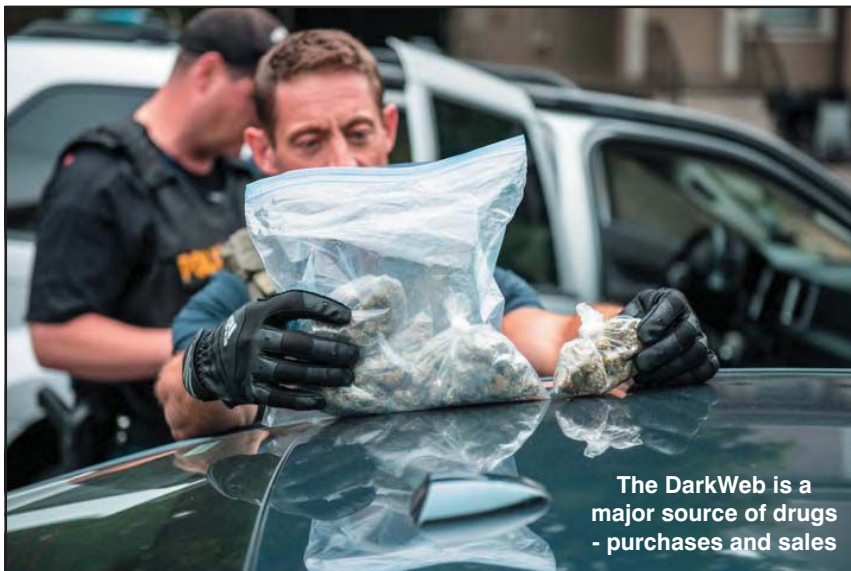


Some websites provide services to monitor people, organisations and systems; others openly claim assassins can be hired - at a price



Those who use the DarkWeb and some of its disturbing and illegal services are increasingly targeted by international security agencies

INTEL: At this time no information was found on the DarkWeb about cyber assassination products or services (targeting medical services etc.). With all that is happening on the DarkWeb, it is only a matter of time.



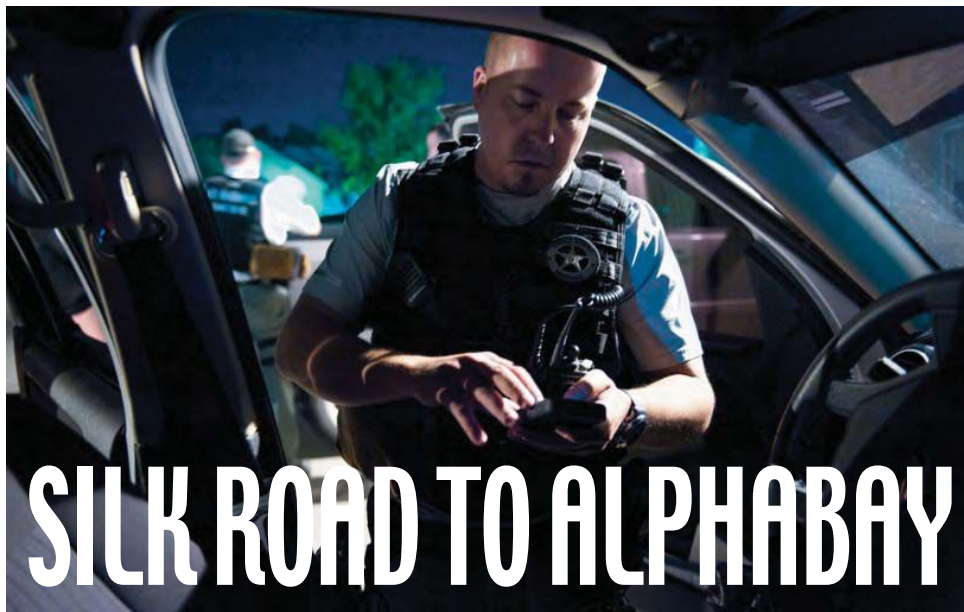
The DarkWeb is a major source of drugs - purchases and sales

OPERATION BAYONET

The secrets of the DarkWeb are many. However, some progress regarding counter-measures is being made. In July 2017, as part of Operation Bayonet, the Federal Bureau of Investigation, Drug Enforcement Agency, Britain's National Crime Agency and Europol took down AlphaBay, the leading market on the DarkWeb.



AlphaBay had over 200,000 users, 40,000 vendors and an estimated \$1 billion in transactions since it began operations back in 2014. This and actions by the Dutch National Police against Hansa (another DarkWeb marketplace) have some asking what's next for other marketplaces on the DarkWeb? However, there are so many marketplaces in operation on the DarkWeb and an incalculable number remain below the radar of intelligence organisations and law enforcement - all continue to operate unabated.



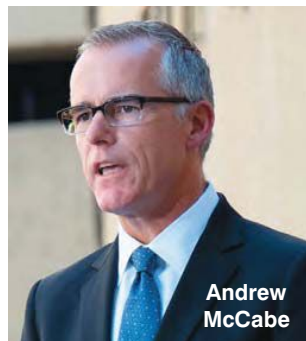
SILK ROAD TO ALPHABAY

Similarities Obvious with Demise of Another DarkWeb Operator

AlphaBay operated for more than two years and had transactions exceeding \$1 billion in Bitcoin and other digital currencies. The site, which operated on the anonymous Tor network, was a major source of heroin and fentanyl, and sales originating from AlphaBay have been linked to multiple overdose deaths in the United States.



Speaking about the international intelligence and security effort (Operation Bayonet) resulting in its closure, FBI Acting Director Andrew McCabe said: "This was a landmark operation. We're talking about multiple servers in different countries, hundreds of millions in



Andrew McCabe



Ross Ulbricht

cryptocurrency and a Darknet drug trade that spanned the globe."

A dedicated team of FBI agents, intelligence analysts, and support personnel worked alongside domestic and international law enforcement partners to shut down the site and stop the flow of illegal goods. "Vendors were shipping illegal items from places all over the world,"



THE DARK WEB

Continued...

INTEL: The actions against AlphaBay and Hansa will undoubtedly be used by those operating on the DarkWeb as a valuable lesson of how not to get 'busted'. Operators will learn from what happened, adapt, plan and move forward.

The DarkWeb is now a haven for rogue-nation-states, illegal resources, criminals and hackers. The items, products and services for purchase, sale or hire are terrifying, and it is not likely to get any better. Intelligence and law enforcement officials continue to express the need for covert operatives who have the skills necessary to infiltrate and monitor the DarkWeb and its growing illicit activities. However, the expansiveness and continued growth of the DarkWeb makes it impossible to have a deep understanding of all its products, services and information contained therein.



What has been covered should provide some understanding of the national security issues and implications of the DarkWeb combined with cryptocurrencies.

EYE SPY WARNING: The DarkWeb is no place for amateurs or those who do not have highly secure computer systems. Whilst it is not illegal to access, we believe it is best not to venture into the DarkWeb.

FURTHER READING: A Rand Corporation article titled: *'The illicit trade of firearms, explosives and ammunition on the DarkWeb'* is recommended reading for additional insights.



US Government exhibit showing nine different identity documents used by Ross Ulbricht

said FBI Special Agent Nicholas Phirippidis who worked on the case

AlphaBay, an outgrowth of earlier DarkWeb sites like Silk Road - but much larger - went online in December 2014. At the time of its closure, the site had more than 250,000 listings for illegal drugs and toxic chemicals, and more than 100,000 listings for stolen and fraudulent identification documents, counterfeit goods, malware and other computer hacking tools,

firearms, and fraudulent services.

By comparison, the Silk Road dark market - the largest such enterprise of its kind before it was shut down in 2013 following an operation codenamed Onymous - had approximately 14,000 listings. Its creator, Ross Ulbricht, who used the pseudonym 'Dread Pirate Roberts' was arrested in 2014, convicted and sentenced to life in prison without the possibility of parole.



DEADLY END GAME OF DARKWEB OPERATOR

On 5 July 2017, Canadian Alexandre Cazes, the 25-year-old founder of DarkWeb site AlphaBay was arrested in Bangkok, Thailand. In addition, his wife was arrested for money laundering. At the time of his arrest investigators valued his personal estate at around \$23 million.

One week later Cazes committed suicide inside his jail cell at the Narcotics Suppression Bureau in Laksi district. He was found dead hanging with a towel around his neck from the ceiling of his cell.

Ironically, the demise of AlphaBay and the arrest of Cazes, came about because of information discovered on his unencrypted laptop and a few undeleted e-mails. From these, investigators built a strong case against the operator.



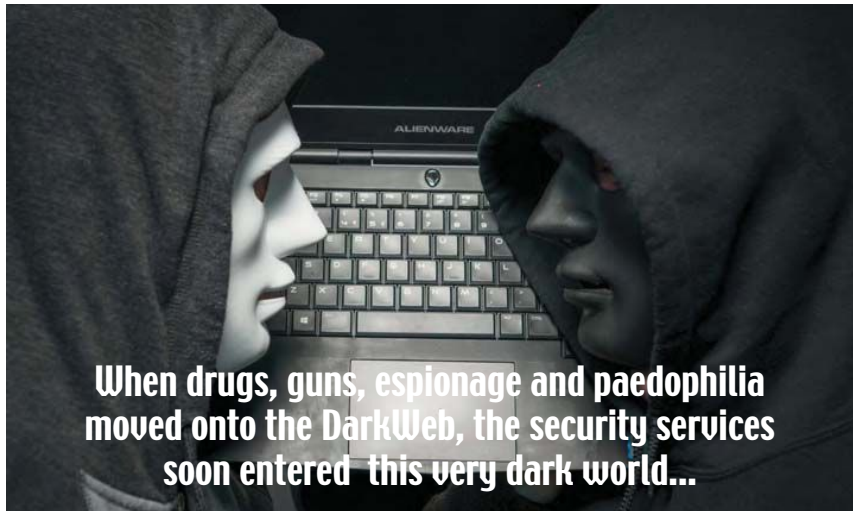
DARK WEB

Law Enforcement Agencies Worldwide Are Fighting Back

GOING UNDERCOVER: Security and intelligence agencies all over the world are deploying techniques to identify and ultimately convict DarkWeb illicit users. Taking advantage of the protections of anonymity offered by browsers like Tor, agents are going undercover to expose operators - you never know the identity of government people.

HACKING: One way to circumvent Tor is to attack the endpoint; that is, the computers of users themselves. The FBI targeted users of a DarkWeb child pornography site called Playpen: the Bureau deployed malware, so that when a user clicked on a child pornography related forum, their real IP address was sent to investigators, revealing their likely location. (The FBI seized Playpen after the administrator had misconfigured the site, exposing its IP address to the normal Internet). As part of the operation, the FBI harvested over 1000 US-based IP addresses, and Europol generated 3,229 of its own cases. ➤





OPEN SOURCE: Even if a criminal's business exists primarily on the DarkWeb, it's likely they will have left digital 'breadcrumbs' - in forum posts or public documents, for example. This helps investigators identify suspects.

MASS SURVEILLANCE: The UK has a dedicated unit for tackling DarkWeb criminal activities, which takes advantage of the country's mass surveillance capabilities. The National Crime Agency (NCA) and Government Communications Headquarters (GCHQ) Joint Operations Cell (JOC) was launched in November 2015, and was initially engaged in online child sexual exploitation. According to a government document: *'Bulk data has supported the disruption of over 50 child sexual exploitation offenders in the UK in the last 30 months alone'*. Because evidence obtained by interception alone is not admissible in UK courts, people caught by this method are unlikely to ever have a chance to contest its legality.

SEIZED DATA: An arrest of a vendor or the seizure of a marketplace can generate a mountain of new leads for investigators to follow. Prominent German vendor Shiny Flakes was recently targeted uncovering a staggering 320 kilos of drugs. Fortunately for investigators, Shiny Flakes had kept a tidy spreadsheet of all orders which is being used to track down buyers, according to local and state police sources.

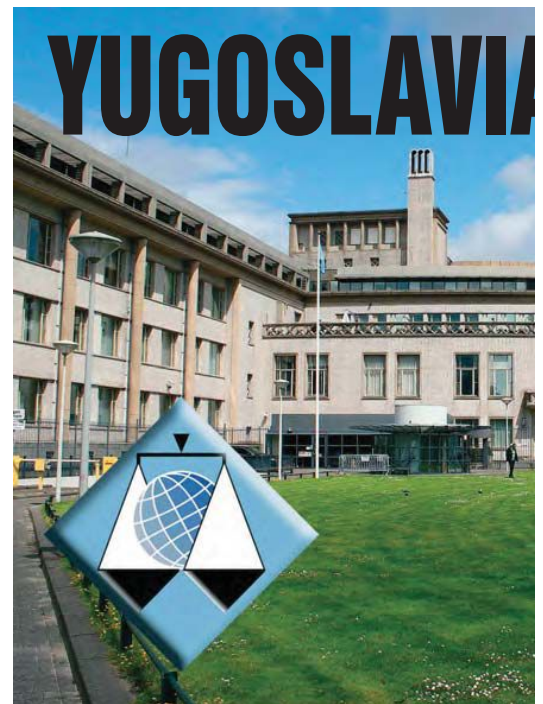
Buying narcotics on the DarkWeb can come back to haunt people years later. After

arresting another vendor who stored details of his customers, German authorities recently fined a seller around £3,000 for purchasing small quantities off the now defunct Silk Road (see sidebar page 40).

TRACKING THE MONEY: DarkWeb marketplaces typically use the pseudo-anonymous cryptocurrency Bitcoin for all transactions, the idea being that transactions can be carried out with no link to the buyer or seller's real identity. US Homeland Security Investigations (HSI), part of the Department of Homeland Security, however, has set up a dedicated task force for tracking down those who launder their proceeds with Bitcoin and other cryptocurrencies.

THE POSTAL SYSTEM: For all its technological sophistication, the DarkWeb illicit trade relies on postal systems and ordinary couriers. Dealers have to properly package products in order to defeat suspicious customs officials who may seize the package. However, once detected, investigators will probe for further details, including the identity of seller and recipient.

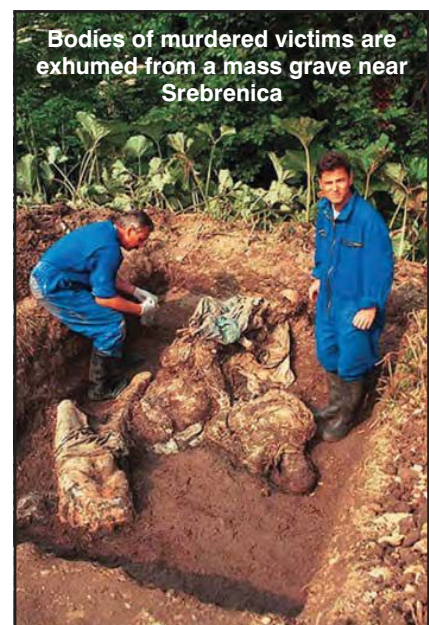
CONCLUSION: Criminals and even those engaged in intelligence and espionage activities always try to stay one step ahead. New technologies have revolutionised how illegal goods are traded or sourced. But when drugs, guns, espionage and paedophilia moved onto the DarkWeb, the security services soon entered this very dark world.



ALTERNATIVE

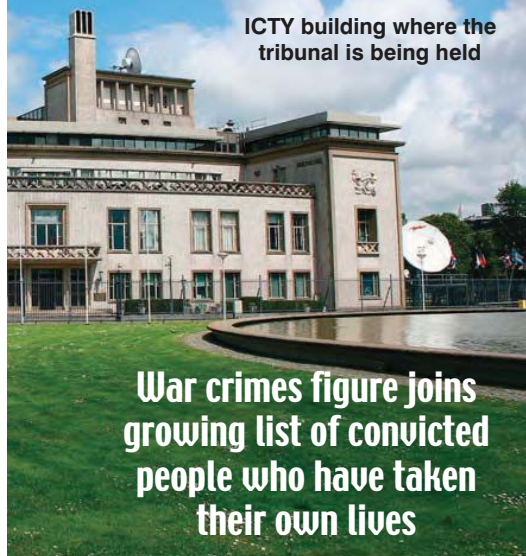
Former Bosnian Croat General Slobodan Praljak, who in 2004 was sentenced to 20-years in prison for war crimes during the break-up of Yugoslavia in the 1990s, committed suicide at the Hague when a judge rejected his appeal. Praljak had already served two-thirds of his sentence, but it appears he could not face serving a further six years in jail.

When the ICTY (International Criminal Tribunal for the former Yugoslavia) judge explained his



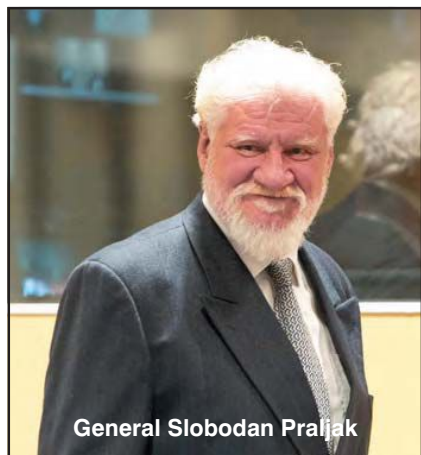
A BREAK-UP

ICTY building where the tribunal is being held



War crimes figure joins growing list of convicted people who have taken their own lives

FIVE OPTION



General Slobodan Praljak

ruling, he shouted "Slobodan Praljak is not a war criminal... I am rejecting your verdict... your contempt," he tilted his head backwards and took a drink from a small vial. He then announced, "I have taken poison." He was taken to hospital but died shortly after.



Slavko Dokmanovic killed himself in 1998



General Slobodan Praljak takes poison as his appeal is rejected

"The preliminary results of the toxicological test showed that Praljak had a concentration of potassium cyanide in his blood," a Dutch prosecution official said. Investigators are still uncertain how he secured the poison, but informed sources have speculated it was smuggled inside a suit he had dry-cleaned for the trial.

General Praljak was a suspect in the long-running UN war crimes trial, and he joins a number of other notorious figures who took their own lives whilst attending the Hague trial. Slavko Dokmanovic had been jailed for genocide and other crimes - he was found hanged in his cell in 1998. Milan Babic, who declared himself the leader of the Serb Republic of Krajina (Croatia), killed himself on 5 March 2006 after being found guilty of crimes against humanity.



Above: Poster of Milan Babic

Perhaps still the most controversial death is that of former leader of Yugoslavia Slobodan Milosevic himself. Mystery surrounds the circumstances

of his demise - by heart attack. He faced a plethora of charges, but was found dead in his cell on 11 March 2006 at the height of the trial. Non-prescription tablets were found in his secure cell and investigators could not confirm he had taken the pills himself. This sparked conspiracy theories.

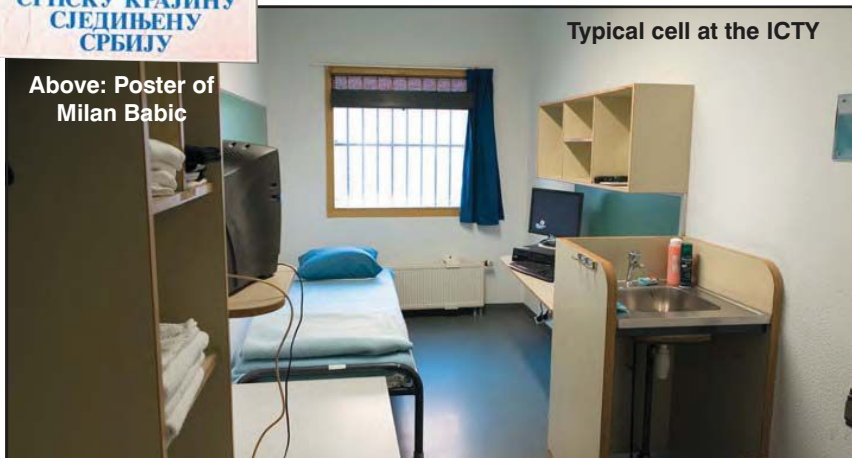


Slobodan Milosevic

Interestingly, in Croatia, Slobodan Praljak still commands a great deal of respect, and in Parliament, ministers and politicians began a session honouring him with a minute's silence. Parliament's President, Goran Jandrokovic read a statement supported by all parties regarding the decision of the Hague: "The [2004] verdict does not honour historical truth, facts and proof... as such it was unjust and unacceptable."

- The ICTY was established by the UN Security Council on 25 May 1993. Since then, 161 people have been indicted

Typical cell at the ICTY



The institution or tribunal is set to close on 31 December 2017

IRAN'S EXPANDING MILITARY INFLUENCE

IRAN UNIVERSAL EXPORTS

US Department of Defense officials have presented convincing evidence that Iran continues to provide weaponry to terrorist groups fighting in Yemen and surrounding areas. In a hangar at Joint Base Anacostia-Bolling, three intact Iranian weapon systems and debris from a fourth, were shown to the media as "proof of covert arming of Houthi rebels." The weaponry was recovered from a number of sites in the region, where fighting forces from Gulf nations, including Saudi Arabia and the UAE, continue to confront terrorists.

The US chose to display the weapons following a missile attack targeting Riyadh



Joint Base Anacostia-Bolling, Washington DC. US Ambassador to the United Nations Nikki Haley discusses evidence of Iran's destabilising activities in the Middle East and its effort to cover up continued violations of UN resolutions. Behind her - various recovered Iranian weaponry

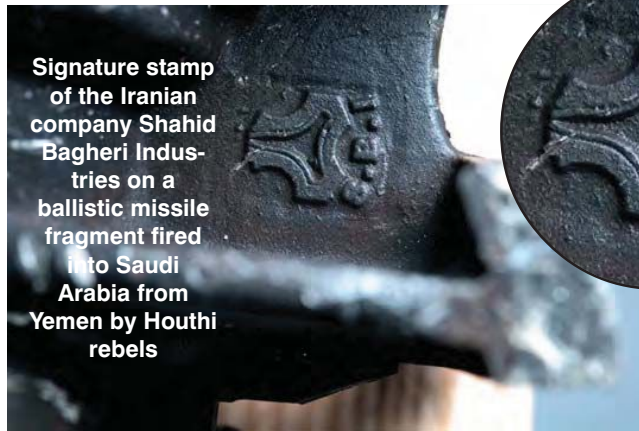
Airport, and is part of a new strategy: "Addressing the totality of Iranian threats and malign activities: nuclear; ballistic missile development and proliferation; counter-maritime operations; cyber; and support to terrorism and unconventional warfare," said Laura Seal, a DOD spokesperson. "Part of the strategy is to show how Iran continues to defy the international community by violating United Nations resolutions."

The weapons systems on display were retrieved from battlefields in the Middle East

by US partners in the region. The four systems are a short-range ballistic missile, an antitank guided missile, an unmanned aerial vehicle and exploding boat technology. "All four include parts made by [the] Iranian government-run defense industry, and all could have only come from Iran," Seal said. Pieces of two Iranian Qiam missiles were shown - both launched from Yemen into Saudi Arabia. One targeted the Yanbu oil facility, the other King Khalid International Airport. "Only Iran makes the Qiam," Seal said.



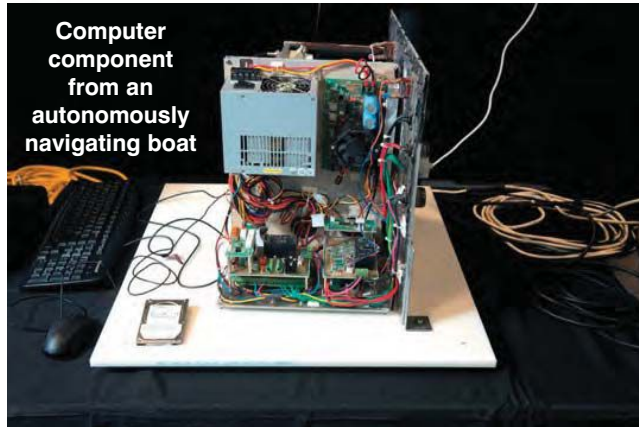
The evidence presented at Joint Base Anacostia-Bolling was compelling



Signature stamp of the Iranian company Shahid Bagheri Industries on a ballistic missile fragment fired into Saudi Arabia from Yemen by Houthi rebels



SHAHID BAGHERI INDUSTRIES



Computer component from an autonomously navigating boat

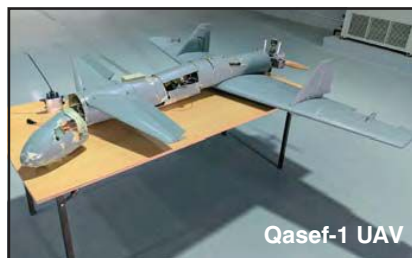


Qiam class ballistic missile fragment

Imagery of recovered Iranian weaponry and technology remnants, including missiles fired into Saudi Arabia from Yemen's Houthi rebels in 2017. They form part of a multinational collection of evidence displayed at Joint Base Anacostia-Bolling proving Iranian weapons proliferation in violation of UN resolutions

Another piece of equipment referenced was an Iranian-made anti-tank guided missile codenamed Toophan. "This was obtained by Saudi Arabia on the battlefield," Seal said. The missile is a high-precision, direct-fire weapon with a range of about 2.4 miles. "The Houthis in Yemen use the weapon to target infrastructure and vehicles," officials said, noting the group does not have the technology to manufacture such weapons.

The display also showcased a Qasef-1 UAV (unmanned aerial vehicle) operated by Houthi forces, which was recovered by Saudi Arabia. "The Qasef-1 can be used as a one-way



Qasef-1 UAV

attack UAV - diving on targets Kamikaze-style and detonating its warhead upon impact," Seal said. "Only Iran makes the Qasef-1. It is a member of the Ababil UAV family, designed and produced by the Iranian government."

The guidance system from an Iranian Shark-33 boat was also featured. This originated from an explosive-laden, unmanned boat used in an attack against Saudi Arabian frigate HMS al Madinah. "What makes the Shark-33 so dangerous is a guidance system allowing it to track and hit a moving target without an operator on board, so the boat can be deployed to blow up a ship without sending someone on a suicide mission," Seal said.

Tehran's role in missile proliferation and backing terror groups has increased since 2015 when it signed a nuclear deal with the West, Russia and China.



Remnant of an Iranian anti-tank missile



Qiam class ballistic missile fragment

SECRET DAESH ACCORD

A database of nearly 26,000 known ISIS fighters has been compiled by 70 nations - many are now returning home

CIA-ISIS Intelligence Back-Channel

A covert deal shielded from media eyes guaranteed ISIS fighters unhindered exit from Raqqa - a deal ensuring many terrorists would live to fight another day...

Following defeat of ISIS in Raqqa, newswires carried reports that Alliance fighters had allowed a few dozen remaining and trapped ISIS operatives to leave the Syrian city, thus ensuring no further fatalities in the battle for the so-called de facto capital of the terrorist group. Since then, all manner of odd reports and stories have emerged, some provided for by intelligence officials and reporters attached to various fighting units.

Perhaps the most concerning and bizarre of all - a disturbing BBC essay that as many as

6,000 heavily armed ISIS terrorists and their families were allowed to leave the city on 10-11 October 2017 in a convoy stretching an astonishing five miles.

Unfortunately for international intelligence agencies engaged in a programme to identify ISIS fighters (in the event they return home), most have since disappeared; some have made their way to other fighting units, hundreds have reached the Turkish border and many have sworn to return to their home nations to continue the fight. A tiny number have been detained.



When Syrian Democratic Forces (SDF) announced 'victory', observers were of the opinion that back-channels of communication had been created between ISIS and government forces. Some of the contacts were cemented by 'third parties', allegedly controlled by the CIA and Russia's GRU. And contrary to the official line that only a handful of ISIS fighters were allowed to depart, the 'tall tale' seems absolutely authentic.



Images from Raqqa show the city has been virtually flattened

The SDF is made up of various fighting units backed and led by US forces



Film footage taken by locals show an organised departure using hired drivers (as insurance against airborne attack) driving a variety of transport, from buses, cattle trucks and vans to ordinary saloons. Their destination was an area in Deir Ezzor Province still under ISIS control.

ISIS IGNORED RULES FOR DEPARTURE

Few intelligence and military personnel were happy, but the secret deal, offered to ISIS heads was made by city officials - and it didn't apply to foreign fighters - who would not be given safe passage - coded speak for detention or worse. And despite assurances that ISIS fighters would depart only with their sidearms, hidden in larger trucks was a cargo of heavy weaponry, explosives and other munitions. Some fighters chose to wear suicide explosives' belts and departed holding their weaponry aloft in plain sight. Intelligence analysts dubbed the operation 'Raqqa's dirty secret', because the entire event was to be kept hidden away from the prying eyes of watching journalists.

"This convoy is not our idea... we did not want a negotiated surrender"



US Colonel Ryan Dillon has acknowledged operation



Film stills from residents of Raqqa and a BBC crew show departing ISIS fighters and their final drop-off point



SDF counter-terrorism unit fighting ISIS

Due to the scale of the operation, and in today's world of instant communication and cell phones capable of recording imagery, details of what really happened during the end game of ISIS activities in Raqqa have emerged. Similarly, it's difficult to stop journalists attached to SDF units from asking leading questions.

The local drivers hired to make good the terrorists escape were offered payment. However, in many cases, and despite participating in a very dangerous enterprise, no monies have been delivered, and now Raqqa's 'dirty secret' is in the open, and many Alliance heads are far from happy. One hired driver explained how ISIS fighters tied IEDs to his truck, while another spoke of



terrorist youngsters deliberately “fitted with bomb vests.” Another was told the convoy would take around 200 fighters to a pre-determined and safe location, but he explained the real total was 4,000, including family members. Throughout its journey, the convoy was monitored by surveillance aircraft and UAVs. And interestingly, during nighttime hours, illumination flares were dropped from the air allowing drivers to see the road ahead.

ISIS’s band of foreign fighters secured their freedom, and checks via the hired drivers have identified numerous foreign nationals - from Britain, France, China, Yemen, Pakistan, Turkey and Saudi Arabia to name but a few. Others spoke “good English.”

Forced to acknowledge that the operation opposed the claim of US Defense Secretary James Mattis, who had said no fighters would be allowed to return to Europe and elsewhere, the heads of Operation Inherent Resolve have now acknowledged the convoy secreted out a large fighting force of terrorists. US Colonel Ryan Dillon said that although an OIR official was part of the back-channel team led by Raqqa Civil Council officials, he did not have input into the “safe passage negotiations.” He insists only a handful of foreign fighters departed and were eventually detained. “In the course of the screening there were four fighters identified by the SDF,” said Dillon. “Of 3,500 civilians, approximately less than 300 were identified and screened as potential ISIS



fighters.” Eye Spy understands of these, biometric data was secured. Dillon also said a register containing the identity of 26,000 fighters had been compiled by 70 nations.

Despite the controversy of allowing a shielded force of ISIS fighters to depart, Eye Spy sources said the entire operation was to limit casualties - both civilian and SDF troops. Major General James B. Jarrard commander of Special Operations Joint Task Force Operation Inherent Resolve, hailed the victory in Raqqa but avoided discussing the secret convoy. “ISIS has no capital or caliphate and is running out of places to hide,” he said. “Their leaders are hiding, Raqqa was freed by Syrians and Syrians will govern Raqqa.” The US has an estimated force of 4,000 troops in the country.

The operation to retake Raqqa, which began in June, had ended. A parting comment was made by an ISIS terrorist to one of the convoy drivers. “Let us know when you have rebuilt Raqqa, we will be back...”

Collusion, Dirty Tricks & Covert Liaisons

THE 30% S

Former MI6 officer who wrote the intelligence-based Trump Dossier concedes some of its explosive content may not be accurate...

A new book titled *Collusion: How Russia Helped Donald Trump Win* by Guardian journalist and Russian specialist Luke Harding threads its way through the many stories linking President Trump’s advisors, backers and confidants, to the powerful political underworld machinery of Moscow. All the usual figures are referenced, including former MI6 officer Christopher Steele, who like many ex-intelligence men and women, now ply their trade in private security.

November 2017. US President Trump in South Korea. He has consistently rejected claims of Russian liaisons and secret meetings



US Defense Secretary James Mattis



SOLUTION



President Putin has sided with his US counterpart and rejected widespread allegations that Moscow secretly helped Donald Trump reach the White House



Ex-MI6 officer and Russian specialist Christopher Steele

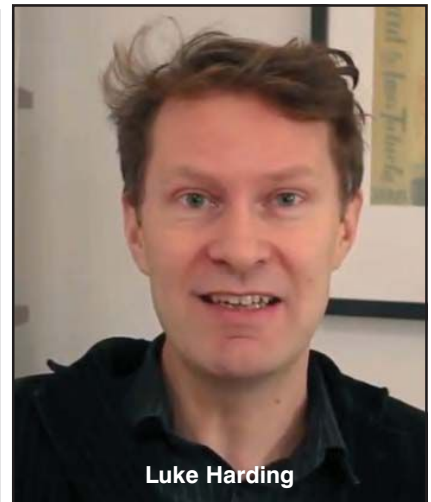
And it's some of Steele's commentary regarding his work on the so-called 'Trump Dossier', that has provoked a stir in journalistic, political and intelligence circles. Steele's provocative investigative findings were made available to FBI and CIA people several months before the 2016 US General Election. For reasons aplenty they didn't surface until after the race for the White House was over. This provoked a major web of conspiracy that has drawn-in so many well known characters and continues to make headlines today.

The reliability of feature segments, including meetings and the behaviour of some characters in the report, has already been dissected, analysed and questioned. Other bits are simply not true. So what's left? On release of *Collusion*, newspapers carried the tag line - 'Christopher Steele Stands by Report' - with a secondary banner - '70 to 90 per cent of report accurate'. "If ever a comment was open to suggestion, then this was it," a former MI6 contact man told Eye Spy. "Which bits are true and which are not?"

These are loaded questions and only Christopher Steele can really apply a qualified answer. President Trump's aides no doubt, believe the controversial and distasteful incidents fall into the percentage section that is questionable. And remove this, then the razor edge of the dossier is blunted.



Former FBI Director Robert Mueller



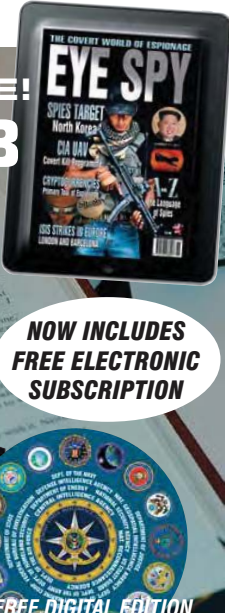
Luke Harding

Nevertheless, Steele stands by his work, and few doubt his past MI6 credentials as a Moscow Desk officer. "I've been dealing with this country for 30 years," he said. "Why would I invent this stuff?" That's not really the point, the author now accepts that not all is truly bona-fide, and intelligence analysts agree that caveats and references should have been inserted in some sections questioning commentary, personalities and dates. Above all, additions, or at least an introductory paragraph or two should have been added regarding the purpose or objective of the report and those sponsors who met *before* its inception and paid for the work. "This would, at the very least have acted as a safety net for Steele," our source said.

Some in the intelligence world have drawn comparisons to a myriad of stories now being labelled 'fake news'. Here too, readers, listeners and watchers of news will find authentic information mixed with and seeping



**FANTASTIC VALUE!
FOR 2018
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.eyespymag.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
ORDER REF: ES-MMUS UK £7.50 USA \$16.00 EUROPE/ROW £8.50

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!

Fantastic clarity - optical friendly



Senator Richard Burr



into less than truthful material - the objective being to surprise, prompt debate and controversy and allow the crux of the story to ferment and cause mistrust. This covert popular intelligence media element has for decades been used as disinformation and propaganda.

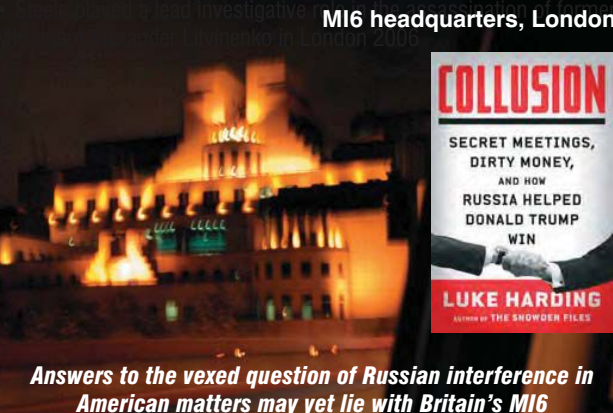
More importantly, and directly related to the Trump Dossier, is Steele's admission that as much as 30 per cent of his report may not be accurate. It is damaging to the credibility of such a highly charged and internationally important work. No doubt the US investigative team probing alleged Russian interference in the US General Election, will have to consider the '30 per cent' issue.

Senator Richard Burr, Senate Intelligence Committee Chairman, has asked Steele to meet his investigative panel probing the dossier, but as yet the intelligence man has not accepted his invitation to Washington. "We have attempted to meet with Steele, but our offers have not been accepted," he said. Another former intelligence officer officially investigating the dossier is ex-FBI Director Robert Mueller, who is acting as Special Counsel. Appointed to probe alleged collusion and interference in the election, he has many 'old friends' in British Intelligence, and it's more than likely if anyone can establish a back-channel, then it is Mueller. The experienced Bureau man has assembled a special investigative team including senior intelligence officers from the FBI and Internal Revenue Service (IRS), plus 14 solicitors.

Also of relevance, in early January 2018, Senate Judiciary Committee Chairman Chuck Grassley and Senator Lindsey Graham passed a classified memorandum to the US Department of Justice (DOJ) relating to communications between Mr Steele and "multiple US news outlets." Both have urged the DOJ to investigate Steele about "the distribution of claims contained in the dossier."

As for Harding, the Russian expert and highly qualified investigative journalist said the material and story surrounding the Trump Dossier is "the most important event of our age... bigger than Watergate." He once lived in Russia and has had his own fair share of run-ins with Moscow. His 2011 book *Mafia State* details his experiences in Russia; he chose to describe the political system under President Putin - 'a *Mafia state*'.

MI6 headquarters, London



COLLUSION
SECRET MEETINGS, DIRTY MONEY, AND HOW RUSSIA HELPED DONALD TRUMP WIN
LUKE HARDING
AUTHOR OF THE SNOWDEN FILES

Answers to the vexed question of Russian interference in American matters may yet lie with Britain's MI6

DARK MONEY, COMMUNISTS & NAZI SPIES

A portrait of a man in a military uniform. He is wearing a dark peaked cap with a gold-colored band and a small emblem. He has light-colored hair and is wearing round glasses. He is wearing a dark green uniform jacket with a high collar and gold-colored buttons. The background is a mottled, earthy tone.

BACKGROUND



Dr Rory Cormac

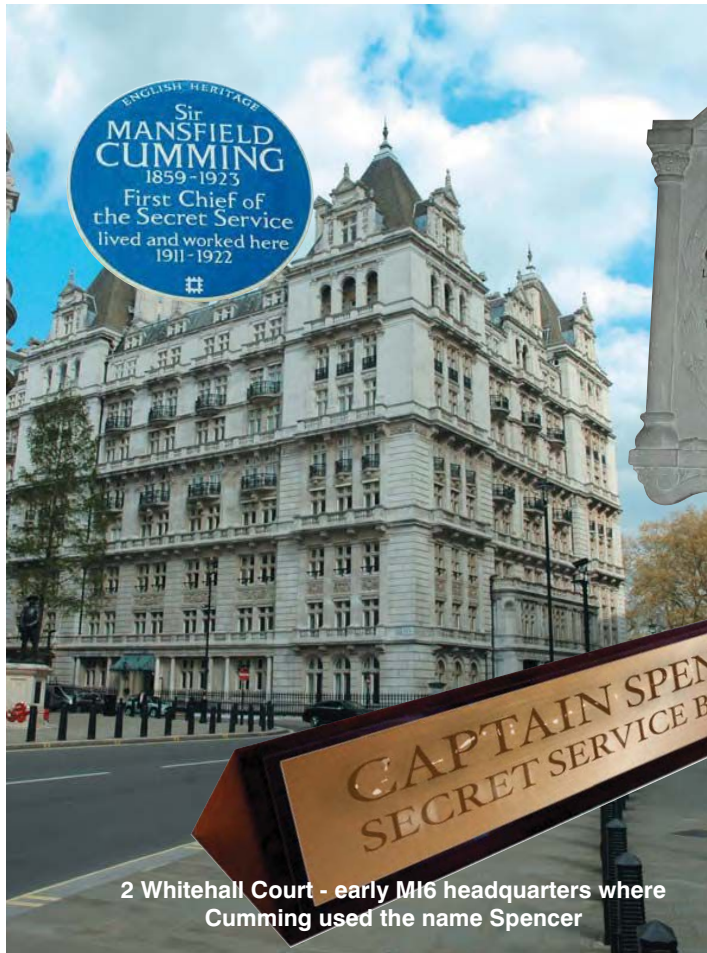
(b) SAVING

1. \$375,000 spent (L.A. 1957) and \$275,000 in July 1957 and \$75,000 in August 1957
2. \$275,000 spent (L.A. 1957) and \$100,000 in August 1957 and \$175,000 in September 1957
3. Leaving \$100,000 in hand for the old authorization, plus \$175,000 from the old authorization (\$150,000)

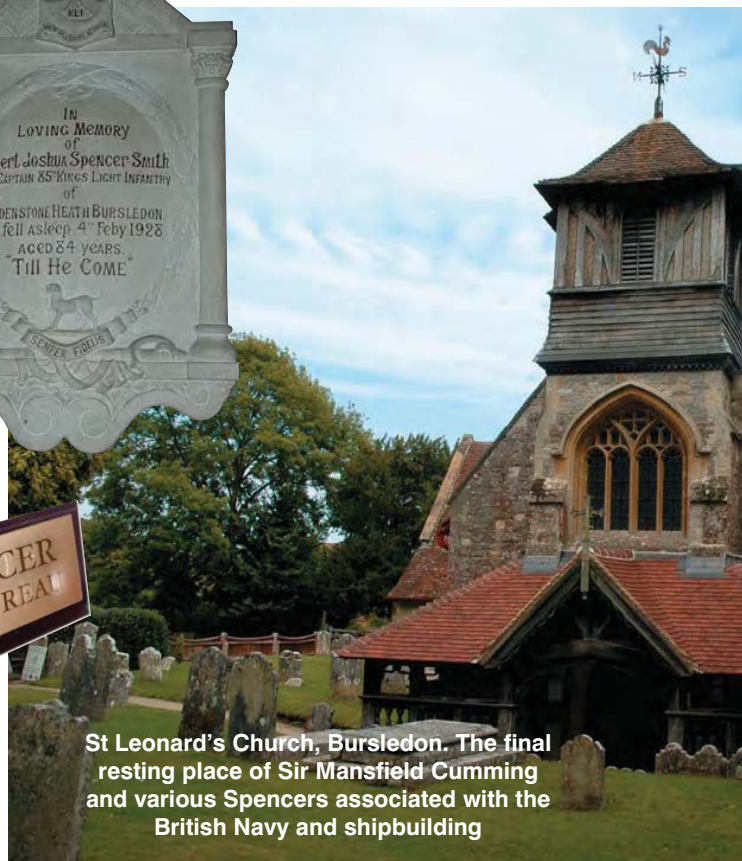
(b) AVALON

1. \$200,000 authorized (\$75,000 now); \$150,000 spent (\$75,000 in July 1957 and \$75,000 in August 1957)

However, what makes the Spencer account unique is that it appears it could only be accessed by Menzies himself; some have speculated it's possible that each time a new M16 Chief was installed, this 'route' to its coffers was passed down. However, Dr Cormac, does not think this is the case with the Spencer account. He told Eye Spy: "I'm fairly confident that this tradition died off with Dick White. He closed the various accounts and formalised reserve spending in a way which probably left little need for the name Spencer." Dr Cormac's discovery is 



2 Whitehall Court - early MI6 headquarters where Cumming used the name Spencer



St Leonard's Church, Bursledon. The final resting place of Sir Mansfield Cumming and various Spencers associated with the British Navy and shipbuilding



Sir Stewart Menzies

therefore significant and revealing. It also throws new light on how Menzies chose to pay for some operations.

DISCOVERY

Details of the account were found in a file from the

Cabinet Secretary's secret and personal archive. It is a record of a meeting in 1952 with Menzies and senior officials from the Treasury and Foreign Office. Sir Stewart was about to step down and hand over the reins of MI6 to Sir John Alexander Sinclair. At the meeting he revealed details of the secret bank account or 'unofficial reserve'.

Permanent Secretary to the Treasury, Sir Edward Bridges said if it was a substantial sum, it might raise questions of accountability: *'The use of such unofficial reserves by 'C' without the prior consent of the Foreign Office, could enable him to carry out policies other than those approved by the Foreign Office and without their knowledge. Clearly this was unlikely to happen, but it would be wrong not to preserve against it'*.



Sir Dick White

Menzies explanation of why the account existed is also documented: *'He thought it right to have a large sum to meet such*

contingencies as (a) a very large inducement to some person in an absolutely key position, or (b) the Vote for the Service being drastically cut in some political emergency in a way which would make it impossible to carry on the Service in the way it was necessary'.

One file contains a list of the secret operations by codename: Avalon, Scant, Scream, Sawdust and Straggle to name but a few. Four represent covert actions in the Middle East. Alongside is the amount spent on each in one year; for example, £200,000 on Sawdust (an operation against President Nasser in Egypt).

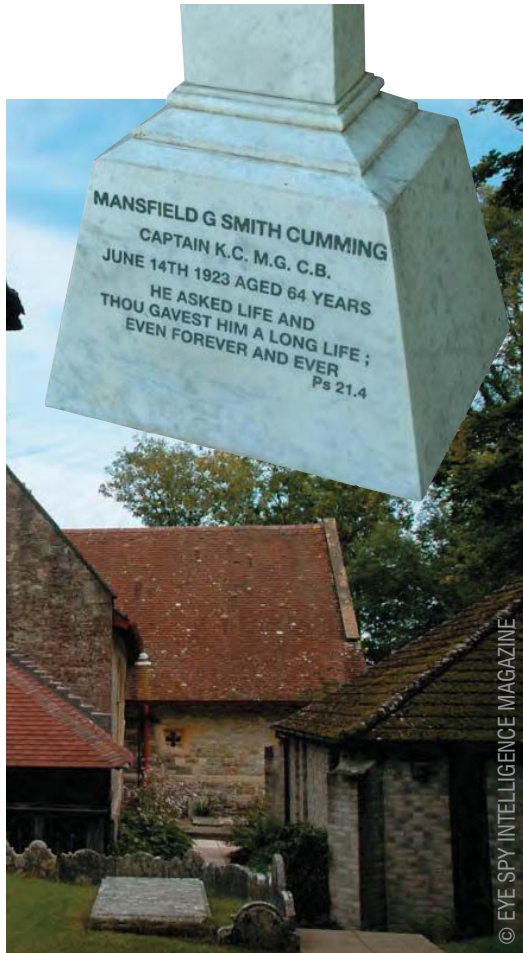
There are also references to some operations involving assassination of senior officials to bring about regime change, though none were conducted.

Last word must go to BBC Security Correspondent and friend of Eye Spy Gordon Corera. "Today, MI6 says it operates under law and careful political and financial control. But if you are ever in a bank and hear someone ask to make a large withdrawal in the name of a Captain Theo Spencer... then let us know."



Sir Stewart Menzies lived in this London building

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



© EYE SPY INTELLIGENCE MAGAZINE



Gordon Corera (right) and Eye Spy Editor Mark Birdsall

- Gordon Corera's report - 'MI6's Secret Slush Fund' aired on BBC Radio 4 and is still available via BBC iPlayer.

Dr Rory Cormac is an Associate Professor of International Relations specialising in Secret Intelligence, Covert Action, and National Security.

Between 2015 and 2017, he held an AHRC Fellowship examining British approaches to covert action, 1945-1968. Rory is a Fellow of the Royal Historical Society and an Associate Fellow of the Higher Education Academy. Before joining Nottingham, Rory worked at the University of Warwick and King's College London.

22 WHITEHALL - HOLT & CO

In the late 1940s, 22 Whitehall, London, was the location of the bank Holt & Co. It was one known location where 'Captain Theo Spencer' (MI6 Chief Sir Stewart Menzies) would withdraw money from his secret account. Holt & Co was established in 1809 by William Kirkland, agent to the First Regiment of Foot. Here too, army agents kept the accounts of army regiments, distributed pay and subsistence, dealt in supplies of clothing, claims for pensions and injury, and provided a general banking business for soldiers and their families.

In 1923, the business was acquired by Glyn, Mills, Currie & Co, but continued to trade separately. In 1939 Glyn, Mills & Co was itself acquired by The Royal Bank of



Scotland, but Holt & Co still continued to trade as a separate entity until the 1960s with military-linked accounts.



Inside Holt & Co. CIRCA. 1917



COURTESY: ROYAL BANK OF SCOTLAND

A NEW PROFUMO AFFAIR? THE NAZI SPY AND BLACKMAIL

Released MI5 files reveal another secret relationship surrounding one of Britain's best known and infamous post-WWII political figures - former Secretary of State for War John Profumo. He of course was a central character in the early 1960s spy and sex scandal dubbed the 'Profumo Affair', involving KGB and British Intelligence contact people. Profumo was forced to resign. The new papers show at the height of the Profumo Affair, MI6 also referenced a Gisela Winegard [Klein] noting her work for German Intelligence.

The declassified papers reveal Profumo was probably the target of blackmail by Gisela who he met in Oxford in the 1930s prior to the outbreak of WWII. They also contain claims made by Gisela's American husband Edward Winegard in 1950, that the couple separated because he discovered 'endearing letters from John Profumo written on House of Commons notepaper'.

In 1951, the Winegards applied for a UK visa but were rejected. An attached note stated:



Gisela Winegard - spy, romancer, model and... blackmailer

© CROWN COPYRIGHT/NATIONAL ARCHIVES

'The 'Winegards had recently engaged in blackmail activities and now think it possible their intended visit to the UK may be connected with this'.

And interestingly, the visa application they submitted listed Profumo as a reference!

SURVEILLANCE

HIGH-QUALITY REAR VISION
SURVEILLANCE SUNGLASSES



**USED ONLY
BY PROFESSIONALS**

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



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

Please use order form on page 82 or visit:
www.eyespymag.com



John Profumo (right)
resigned following a
sex and spy scandal

© CROWN COPYRIGHT/NATIONAL ARCHIVES

EDITOR'S COMMENT: It should be noted that Profumo actually advised MI5 around 1941 that he knew Gisela from the 1930s; and that the papers reflect suspicion from at least one of his associates. This probably surrounds an affair she had in 1938 with a senior German Army officer based in the German Embassy, Paris. Gisela was arrested in 1944 following the liberation of the city by Allied forces.

SIR KINGSLEY AMIS MI5 EYES ON A SECRET COMMUNIST?

Newly released British Intelligence documents reveal Sir Kingsley Amis, one of Britain's best known writers, was probed by MI5 shortly after Germany was defeated in WWII, for his 'left-leaning' (Communist) mannerisms and politics while serving in the Royal Corps of Signals.

MI5 discovered he joined the Communist Party as an Oxford student and was a 'recipient of Communist literature and a very promising member of the Oxford Branch of the Communist Party' the documents show. The file has been likened to numerous others surrounding Establishment fears of the secret growth of Communism in Britain.

Other entries note his liaisons with senior figures at the Communist Party newspaper the *Daily Worker*.

The material shows MI5 continued to surveil the writer, but in actuality, investigators acknowledged he never hid his socialist views and they did not consider him a national security risk. Indeed, his views are said to have changed following the Soviet invasion of Hungary in 1956. A year later he wrote to the *Daily Worker* stating he 'utterly rejected Marxism'. A decade on, Amis even signed a letter to the *London Times* showing his support for US forces fighting in the Vietnam War.

The analysts of MI5 were proven right in their belief that Amis should not be bracketed with other prolific Communist-friendly figures, including those spies belonging to the infamous KGB-operated Cambridge Spy Ring.



Sir Kingsley Amis

CHRISTINE KEELER

London Socialite
Passes into Spylore



Just a week-or-so following release of documents surrounding John Profumo and Nazi spy Gisela Winegard, one of the women at the centre of the later 1960s Profumo Affair, Christine Keeler, 75, passed away. Her London socialite life and affairs with Profumo, Russian diplomat and military attache Eugene Ivanov, plus MI5 contact man Stephen Ward and other Establishment figures have been well documented. Suffice it to say, the scandal almost toppled the Harold Macmillan government of the day.

Keeler's early 2000s memoir *The Truth at Last*, is truly an engaging book revealing the



MI5 contact man Stephen Ward committed suicide in 1963



Russian intelligence officer Ivanov and Stephen Ward met in this London building where they frequently played cards together

background and inside story of many events associated with this period, and also provides a better personal understanding of the central characters involved. However, there have been so many films, plays, books, radio and television documentaries on the spy scandal, that her work and honest reflections have been strangled and consumed by intelligence historians, playwrights and authors. Many believe the book did not receive the acclaim it should have.



One MI5 agent who knew Christine Keeler personally during the 1960s, told Eye Spy editor Mark Birdsall, that she was regarded as an "intelligence source and a person of interest." Not for her work, but for her lifestyle and associates. Her friend, Stephen Ward, osteopath to many famous people, including Winston Churchill, Frank Sinatra and Elizabeth Taylor, to name but a few, killed himself just before he was due to be sentenced for his involvement in the murky business, though a charge of 'living off immoral earnings' hardly suits the tale. "Ward was MI5," said our source. "Not an officer, nor an agent, but he passed commentary and materials to the Service - not just our's, but sadly, probably the KGB as well."

One well publicised task reportedly linked to Keeler was securing information on nuclear missiles and

placement silos in Europe - this by liaising with the likes of Profumo and Ivanov. If this is true, then her bedroom and secret liaisons were not just social, but perhaps purposeful. "She knew exactly what she was doing," our source said.



MI5 Director-General Sir Roger Hollis

Continued on page 82



Eugene Ivanov



The story of Stephen Ward and the Profumo Affair was made into a musical

OUT OF TIME



Paul Rosbaud

THE SPY WHO 'SAVED THE WORLD'

Eye Spy Associate Editor Peter Matthews explains how a hesitant Hitler, a fragmented scientific community, plus the secret work of an MI6 spy and the Special Operations Executive, stopped Germany securing the one weapon which could have turned the tides of war in its favour

Britain's Prime Minister Winston Churchill had nightmares in the early months of WWII concerning uncertainty of what was happening in the race to develop nuclear weapons with Nazi Germany. This was because in the 1920s, Germany had developed and fostered a burgeoning German scientific community giving them a head start in advanced weapons research.

Its armed forces could also call on many of the world's most outstanding physicists, one of whom was Professor Otto Hahn.



Professor Otto Hahn

THE URANIUM SOCIETY

Hahn began his career in the laboratories of New Zealand-born Ernest Rutherford in Cambridge, the father of modern nuclear physics, who first split the atom but then dismissed the possibility of creating an awesome source of energy from it as "pure moonshine."

Within a couple of years Hahn, working in the Kaiser Wilhelm Institut* in Berlin, published a paper containing the theoretical basis of how to release the awesome power of the atom. Following Hahn's paper over 100 other scientists and academics (mainly Germans), published papers discussing ways to split the atom; one of whom coined the phrase 'Nuclear Fission'. Thereafter, more than 70 German scientists gathered together in Berlin to form the Uranverein (Uranium Society) to research the subject.



By Peter Matthews

As the clouds of war gathered, Jewish physicists wisely chose to flee Hitler's Germany. They came to Britain and America to work which weakened the intellectual power of Uranverein Society, among the emigres was one Albert Einstein.

Target of Operation Musketoon - Glomfjord power station. The first attacking force suffered one casualty; the second group were not so fortunate - seven SOE men were captured and later executed. Right: Glomfjord village today



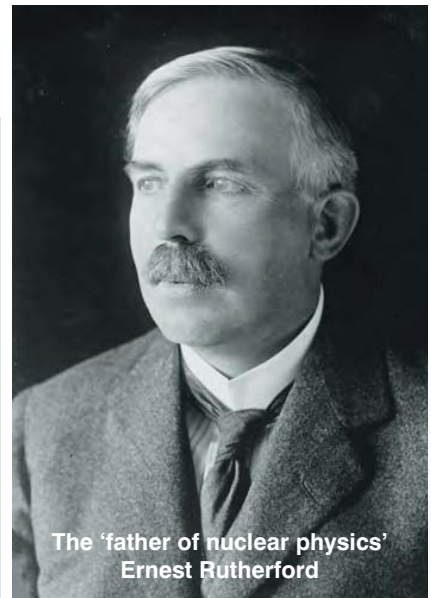


**Atomic bomb explosion
- Nagasaki 1945**

some of the projects supporting the research programme.

Although the nuclear endeavour was secret, the MI6 spy was able to report that a shortage of materials and resources were a problem for Germany's nuclear programme - specifically heavy water and Uranium isotope separation capability together with an Uranmaschine or nuclear reactor.

As war progressed, gradually the components of the programme came together although each project was harassed by RAF British bombers, particularly a processing facility for heavy water in occupied Norway. The material was needed to moderate the chain reaction in an atomic pile. The construction of the reactor

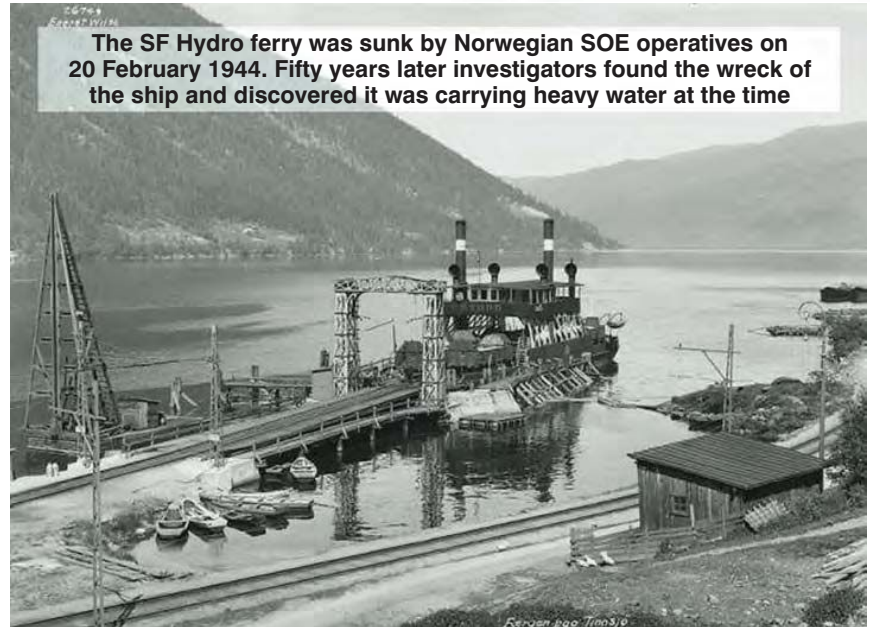


**The 'father of nuclear physics'
Ernest Rutherford**



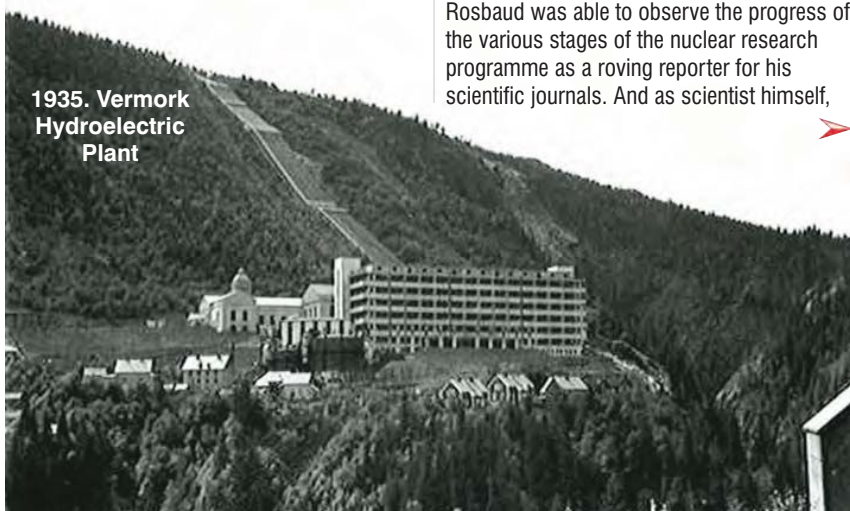
Einstein and Oppenheimer

Before the war in February 1939, members of the Uranverein Society advised the German Ministry of War that Nuclear Fission had the potential for creating a fearsome military weapon. And the Nazi atomic weapons programme would have been a secret but for British spy Paul Rosbaud run by MI6 Berlin Station Chief Frank Foley who monitored its progress. Rosbaud was a reporter for a German scientific publication and knew nearly all the scientists in the Uranverein Society and



The SF Hydro ferry was sunk by Norwegian SOE operatives on 20 February 1944. Fifty years later investigators found the wreck of the ship and discovered it was carrying heavy water at the time

was also delayed by a shortage of steel. And another prime reason for delay was that many German scientists were actually being called up for active service by the Wehrmacht. Rosbaud was able to observe the progress of the various stages of the nuclear research programme as a roving reporter for his scientific journals. And as scientist himself,



**1935. Vermark
Hydroelectric
Plant**



MI6 Station Chief Frank Foley



Left: Reconstruction of Operation Gunnerside team preparing to destroy a cascade of electrolysis chambers at Vermork Hydroelectric Plant. The SOE agents have made the German plant employee turn away as they assemble the charges

he was able to understand the technology involved.

The intention of both sides to develop a bomb was an open secret; *The London Times* carried an article in May 1940 reporting that Berlin had ordered German physicists to concentrate on Uranium oriented research.

In spite of the newspaper report, British Intelligence had no real knowledge or insight

into the actual progress of the German atomic bomb project, or what had been achieved thus far. So MI6 went into overdrive. Rosbaud was the organisation's primary source so they decided that the best intelligence strategy was for him to keep track of the movements of the various members of the Uranium Society.

In London, British scientist R.V. Jones was able to maintain a watch on many German scientists. One in particular, Werner

Heisenberg, was making the most progress so MI6 considered assassinating him. Ultimately analysts decided that the movements of the leading German physicists showed they were not associated with any large-scale construction projects - the kind needed to operate and construct an atomic bomb. However, they also concluded that there "were many worrying indications that Germany was making progress."

OPERATION MUSKETOON

Rosbaud sent his reports to London through couriers of the Norwegian underground XU network (X - Unknown U - Undercover) who passed them through neutral Sweden. One secret report alerted the Special Operations Executive (SOE) that a large amount of heavy water was to be moved from the Norwegian processing facility in Vermork.

It led to the SOE's successful Operation Musketoon in which the German-operated Glomfjord power station in Norway was targeted (September 1942). Two years later, and following various attacks on the facility and its support system, the ferry SF Hydro,



1913. Otto Hahn at the Kaiser Wilhelm Institut in Berlin



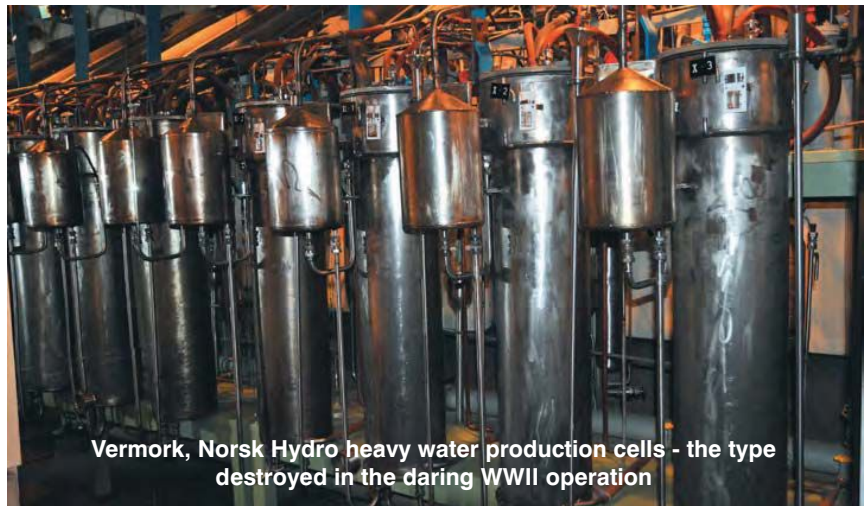
Julius Robert Oppenheimer



Werner Heisenberg. MI6 considered assassinating the scientist

carrying a large cargo of the material, was sabotaged and sunk in Lake Tinnsjø. The incident became the subject of a film after the war starring Kirk Douglas. Another Norwegian heavy water facility, the Vermork Hydroelectric Plant was also targeted under the auspices of SOE's Operation Grouse, Freshman and Gunnerside.

MI6 concluded from its intelligence that the German nuclear programme was lagging behind the Anglo-American endeavour, but Allied scientists were still nervous, the closer the Germans got to solving the problems the simpler they seemed. The intelligence men began to relax but the scientists remained on edge as the solutions appeared so simple in



Vermork, Norsk Hydro heavy water production cells - the type destroyed in the daring WWII operation

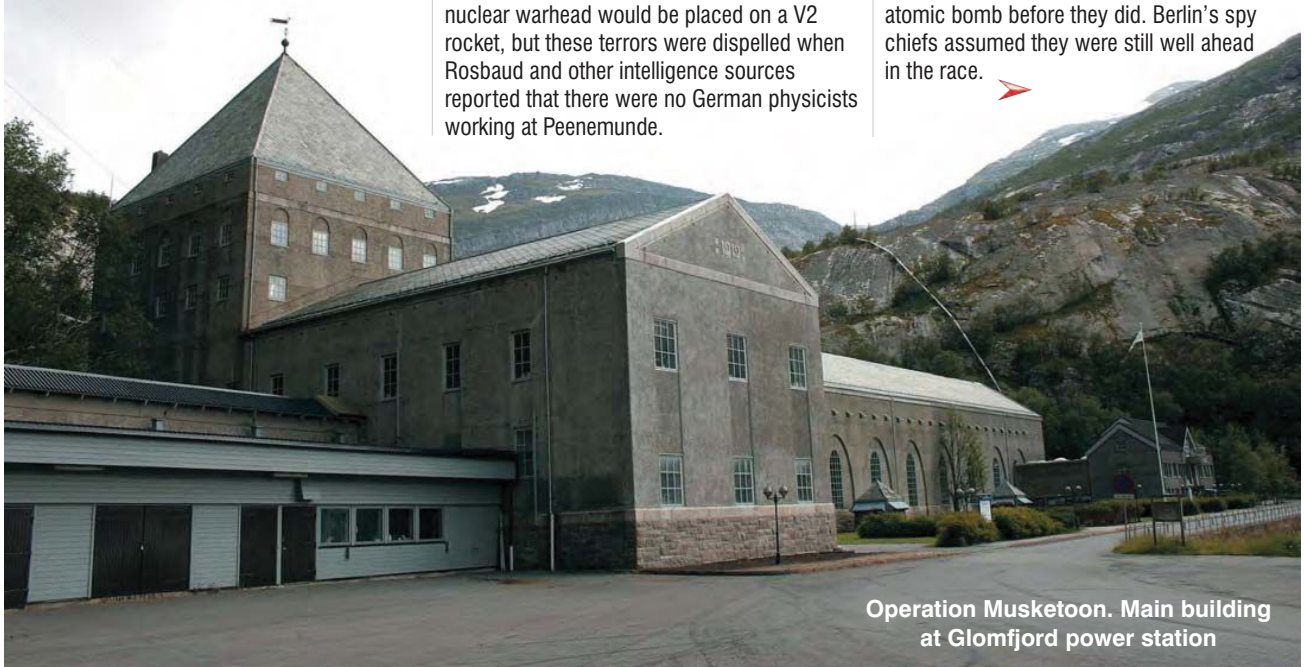


Nuclear reactor replica in the Atomkeller Museum, Haigerloch

retrospect - so why had the Germans not thought of them?

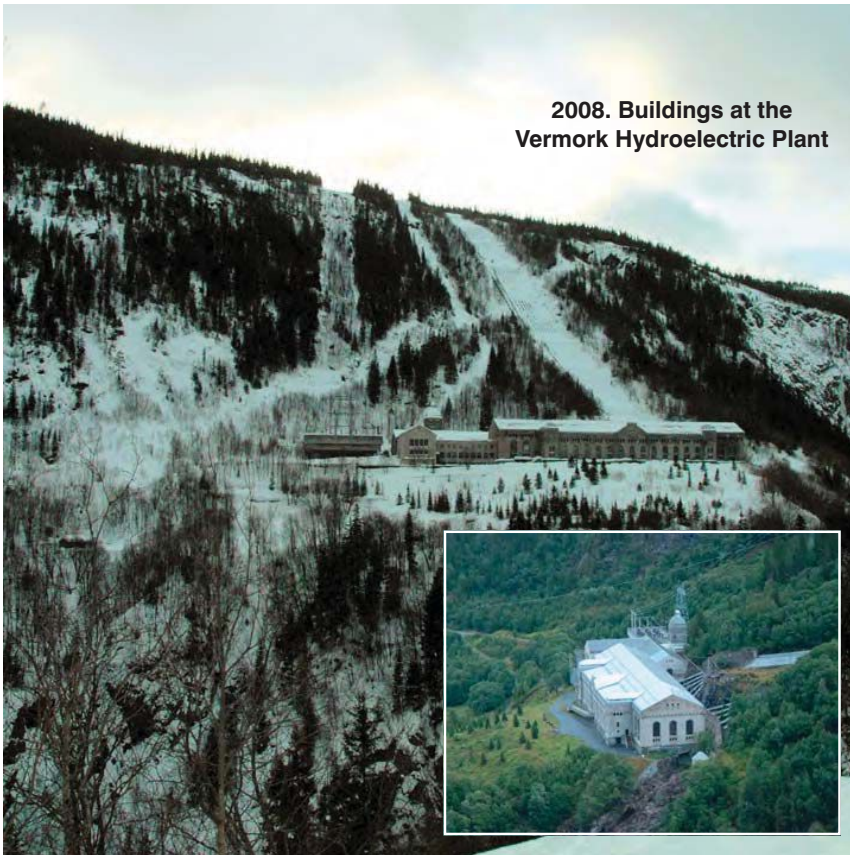
Allied scientists feared that sooner or later a nuclear warhead would be placed on a V2 rocket, but these terrors were dispelled when Rosbaud and other intelligence sources reported that there were no German physicists working at Peenemünde.

The Abwehr (German Intelligence) had no knowledge of the American ALSOS nuclear programme at Los Alamos so they discounted the possibility of the Allies producing an atomic bomb before they did. Berlin's spy chiefs assumed they were still well ahead in the race. ➤



Operation Musketoön. Main building at Glomfjord power station

2008. Buildings at the
Vermonk Hydroelectric Plant



Albert Speer

programme contained many Jewish physicists one of which was Albert Einstein. Research efforts were further divided into different locations working on various aspects of the problem with little communication between them unlike the American method. The US ALSOS programme concentrated their teams all in one place and conducted an integrated research programme under one inspired leader, Julius Robert Oppenheimer.

OUT OF TIME

Hitler appointed Albert Speer as Minister for Armaments and Ammunition later in the war. Speer was neither a scientist nor a military man, and bizarrely decided to close down Germany's nuclear research project and its development of the bomb.

Rosbaud informed London of Speer's decision to the great relief of Churchill, his war planners and intelligence chiefs, as all believed that the only way Germany could have won the war at that stage was by dropping an atomic bomb.

After the war both Operation's Big and Paperclip* [securing the services of selected Germans, including members of its scientific community] revealed the Third Reich's shortcomings (and achievements) in nuclear research and their lack of leadership in the race to make a bomb.

As for MI6 agent Paul Rosbaud, he moved to London and joined the Robert Maxwell Group of companies where the author of this article also worked for some years.

Rosbaud's intelligence had dispelled anxiety about the German atom bomb and helped to delay its completion (with the help of the RAF) for which he was awarded a medal for 'service other than research to physics' by the American Institute of Physics. In its presenta-



Former Kaiser-Wilhelm Institut in Berlin
where nuclear fission was first detected

Germany failed to keep up in the nuclear race for a number of reasons; the overriding one was complacency, lack of focus and bad direction of effort. The situation can be compared to the intelligence and code-breaking work at Bletchley Park.

The German intelligence network used two security services often working against each other; her nuclear programme was even more divided with nine technical sectors which lacked a unified direction. Hitler did not trust his intelligence people, nor to some extent the scientific community, as the nuclear



US and British army specialists at the experimental nuclear pile in
Haigerloch, southern Germany

tion ceremony, Rosbaud was called "the man who saved the world." Certainly he was one of MI6's most important (and unsung) agents of the Second World War.

* Peter Matthews played a role

ABOUT THE AUTHOR: PETER MATTHEWS

is a recognised intelligence historian and Secretary of the Foreign Press Association. He is author of *SIGINT: The Secret History of Signals Intelligence in the World Wars and House of Spies*. After WWII, he worked on various intelligence-related projects in post-war Berlin and elsewhere.



Opening of the Kaiser-Wilhelm Institut in Berlin in 1913. R-L: Adolf von Harnack, Friedrich von Ilberg, Kaiser Wilhelm II, Carl Neuberg, August von Trott zu Solz

THE LIVES OF OTHERS

SOE Exploding Rats and WWII Assassins Tools

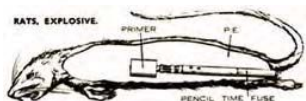
One of the most interesting covert attack objects ever conceived by Allied Special Forces (SOE and OSS) in WWII, was the 'explosive rat'. Few of these objects survive, thus when one was auctioned at Bonhams in New York in December, there was much interest.*

The device, invented in 1941 by the Special Operations Executive, can be likened to an early IED (improvised explosive device) and was intended to destroy enemy boilers. The rat, skinned and packed with plastic explosive had a fuse wire attached.

The idea was to conceal the rat in a coal bunker or next to the boiler. The thinking being, once the animal was discovered, it would be thrown into the fire to destroy it, or inserted along with the coal



French Resistance garrote wire



and then explode - destroying machinery.

However, they were never used operationally, for a batch of around 100 sent to agents for use in mainland Europe quickly fell into the hands of the Germans. Thereafter, they were regularly displayed at German military schools as training exhibits in covert warfare.



French Resistance and SOE officers in 1944



The shaved exploding rat and pen concealing a spike

Nevertheless, the SOE were satisfied because thereafter, searches for explosive rats continued throughout the continent, the Germans incorrectly assuming batches had been distributed to resistance and other covert forces.

The rare surviving example sold in New York belonged to SOE operative Jack Dickens who used the pseudonym Maurice Ledain. He was dropped in France in WWII as part of a sabotage operation, but for reasons unknown, the rat which he was carrying ended up in a French Police station storage unit.

Other auctioned covert devices from the period, included a French Resistance pocket-sized wooden coffin containing a garrote wire for strangling an opponent, and



Another exploding rat sold by Bonhams - note tag - SOE Station XV



an OSS pen which concealed an assassin's spike.

A Bonhams spokesman said: "Some of the disguised weapons are chilling, but they highlight the do-or-die nature of SOE agents who operated in Nazi-occupied Europe."

*The exploding rat sold for \$2125 (£1,590)



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 £34.00 ☐

UK 2 YEARS £55.00 ☐ USA 2 YEARS \$96.00 ☐ EUROPE/ROW 2 YEARS \$63.00 ☐

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



ELECTRONIC

German Intelligence identify would-be Chinese spies who are using modern technology in conjunction with an historical tradecraft

The domestic intelligence agency BfV (Bundesamt für Verfassungsschutz), spent much of 2017, analysing numerous professional and social media accounts of Chinese nationals on business websites such as LinkedIn. The user profiles, complete with stylish imagery and work titles, ranging from consultants, headhunters, scholars and political experts, were all bogus. "The people are little more than ghosts, they don't exist," one intelligence source said. "The ultimate objective is to recruit informants and place its own spies in vital areas to source high-end information, especially from government areas."

The BfV consider the LinkedIn operation an endeavour created and managed by Chinese



BfV
Director
Hans-Georg
Maassen



INFILTRATION



Intelligence to target ten thousand German professionals, in an attempt to infiltrate businesses, government offices and high-end technology companies. "To add credibility to the profiles, they have turned to the old spy ruse of cover and legend - creating complete fake work records, contacts, friends, family and social background."

German intelligence officials have urged its nationals using professional sites such as LinkedIn to be cautious. BfV Director Hans-Georg Maassen said the Chinese operation amounted to a plot to "subvert German politics at a high level." He believes the primary targets are politicians, think tanks



The BfV created a special task force to analyse accounts of fictitious professionals created by Chinese Intelligence who targeted 10,000 German nationals

and major industry figures. "This is a broad-based attempt to infiltrate in particular, parliaments, ministries and government agencies," he said. To provide evidence of the operation, the BfV published the names of some of the 'ghosts' - 'Lily Wu' - a think tank professional based in eastern China, for example.

In its annual report, the BfV identified China as the primary culprit in sourcing German secrets and government policy: *'The focus of Chinese intelligence activities is shifting towards political espionage. They are now trying to obtain more information about supra-national entities such as the EU and G20'*. There was also a reference to the territorial disputes continuing in the South China Sea region.

China naturally dismissed the spying allegations. "Claims we are targeting German nationals are groundless," said the country's Foreign Ministry spokesman Lu Kang. "We hope the relevant German organisations, particularly those government departments [BfV] can speak and act more responsibly." He warned the allegations do little to help bilateral relations.

Linkedin spokesman Billy Huang said: "The safety and security of our platform is always a top priority. We will deactivate any bogus accounts."



Lu Kang

Despite Beijing's rebuke of German Intelligence, the BfV warning complements recent findings of the CIA identifying a major programme to place Chinese nationals (professionals) in key technology and defence companies as part of a long-term espionage endeavour. Similar warnings have been issued by a number of European companies. Australia is already debating new laws after concerns about Chinese activities in universities.



Embassy of China, Berlin



China Ambassador to Germany Shi Mingde



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

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

VOLUME 9

VOLUME 10

VOLUME 11

VOLUME 12

VOLUME 13

VOLUME 14



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



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



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



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



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



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



ISSUE 108 REF: ES/108
UK £3.95 USA/ROW \$7.00



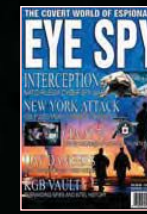
ISSUE 109 REF: ES/109
UK £3.95 USA/ROW \$7.00



ISSUE 110 REF: ES/110
UK £3.95 USA/ROW \$7.00



ISSUE 111 REF: ES/111
UK £3.95 USA/ROW \$7.00



ISSUE 112 REF: ES/112
UK £3.95 USA/ROW \$7.00

YOUR BRIDGE TO THE COVERT WORLD OF ESPIONAGE

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

EYE SPY 17 YEARS OF PRODUCTION!

• 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!

COMMAND & CONTROL

Do the President's Tweets Really Help the Intelligence Community?

Most US intelligence officers have failed to embrace the 'tweets' of President Trump, especially those with a political, security or intelligence agenda - regardless of their content. And privately, a large percentage believe they are damaging - a recent example being his re-tweeting of far-right UK videos and information tabs attacking Muslims. The result was a diplomatic spat between the two allies forcing premier Theresa May to say it was "wrong of the president to have done this."



However, in a strange turnaround, CIA Director Mike Pompeo, speaking to a defence gathering in California, said that in some cases they actually provide the Agency with important information. "How so?" a delegate asked. D/CIA Pompeo responded: "I've actually seen it help us. Things the president has put on his Twitter account actually have a real-world impact on our capacity to understand what's going on in other places in the world."

"That is, our adversaries responded to the tweets in ways that were helpful to us to understand command and control issues, who is listening to what messages, how those messages are resonating around the world."

Other intelligence figures remain unconvinced. One official who spoke on the condition of



anonymity said: "Calling NK leader 'rocket man' and 'short and fat' is not helpful when the CIA is trying to establish back-channels of dialogue with the rogue nation to stop its nuclear ambitions." Former D/CIA Leon Penetta agreed, and said, "...you don't just roll



"Things the president has put on his Twitter account actually have a real-world impact on our capacity to understand what's going on in other places in the world..."

Director CIA Mike Pompeo



Robert Mueller and Michael Flynn

2017. President Trump visits MacDill AFB, Florida. Far left is National Security Advisor Michael Flynn. The president remains supportive of Flynn and has attacked Robert Mueller's Special Counsel probe, asking why the FBI is "out to destroy" Flynn yet has done nothing about claims "Hillary Clinton lied about" e-mail usage





March 2017. FBI Director James Comey visits McEntire Joint National Guard Base, South Carolina. A Special Counsel headed by another former Bureau Director Robert Mueller, has now asked that all e-mails and documents connected to Comey's firing by President Trump in May, be handed to his investigators

a grenade in the room and have things blown up, then not have a strategy for how the hell you deal with it."

And the president could not help enter the debate over the FBI's continued probe into Russian meddling in US affairs. This follows news that former Trump National Security Advisor Michael Flynn has pleaded guilty over his conversations with Russian officials. The special investigative counsel has charged him with lying to the FBI. Flynn has now agreed to cooperate with investigators as part of a plea agreement, a move which upset President Trump who tweeted: 'After years of Comey [James Comey former FBI Director who the president sacked in May], with the phony and dishonest Clinton investigation (and more), running the FBI, its reputation is in tatters - worst in history! But fear not, we will bring it back to greatness'.



Michael Flynn (circled) sits next to President Putin at the 2015 RT dinner in Moscow



2013. Former D/CIA Leon Penetta gives a farewell speech at King's College, London

FBI END OF WATCH

Since its formation in 1908, a total of 67 agents and Bureau professionals have been killed in line of duty. This figure does not include others attached to the organisation, or those killed in non-official and/or covert/secret operations not fully understood or officially recognised or disclosed.



The first FBI agent to die in service was Special Agent Edwin C. Shanahan (left) on 11 October 1925. He was shot by Martin J. Durkin, a car thief who had previously wounded four police officers in an attempt to avoid capture in Chicago, Illinois.



The last reported deaths of Bureau agents in line of duty were Steven A. Carr and Wesley J. Yoo. Both were in the Pentagon when hijacked American Airlines Flight 77, commandeered by terrorists crashed into the building on 11 September 2001. The agents suffered various injuries (exposure to hazardous materials and toxic air) and thereafter illnesses attributed to the attack or made worse. Despite receiving extensive medical support and treatment, the officers passed in September and October 2015.



Wesley J. Yoo



Wreath and memorial for fallen agents within the courtyard of FBI headquarters, Washington DC



Thomas O'Connor - FBIAA head

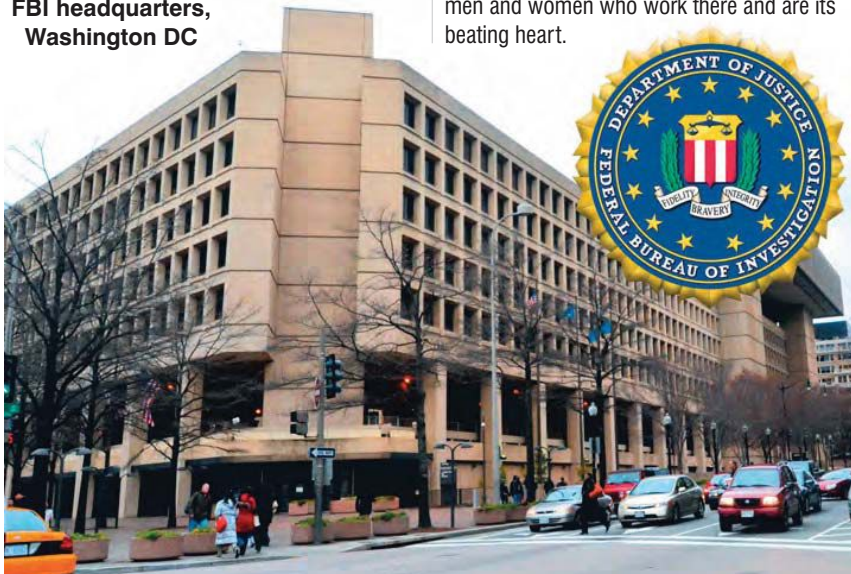


The tweet was met with utter dismay in the corridors of this famous intelligence and security organisation. Questioning the honesty of an officer or even a

director's integrity is one thing, but calling its entire structure flawed is another.

"In reality, the use of expressing personal opinion regarding matters of national security on the Internet is not helpful," a serving US intelligence officer told Eye Spy. "After all, it's the agencies and heads who are then questioned and ultimately forced by the media and observers to provide some sort of reasoning. And it cannot help confidence in the ranks and file." Forced to respond, Thomas O'Connor, head of the FBI Agents Association (FBIAA) said: "Every day FBI Special Agents put their lives on the line to protect the American public from national security and criminal threats. Agents perform these duties with unwavering integrity and

FBI headquarters, Washington DC



The White House letter advising Comey he had been sacked

professionalism and a focus on complying with the law and the Constitution.

"This is why the FBI continues to be the premier law enforcement agency in the world. FBI agents are dedicated to their mission; suggesting otherwise is simply false."

Less than forty-eight hours after the exchange, ex-intelligence man James Comey himself used the Internet to post a cryptic

FBI DIRECTOR DEFENDS ORGANISATION

PRESIDENT'S MAN REJECTS WHITE HOUSE CRITICISM

Current FBI Director Christopher Wray was President Trump's personal choice. Appointed on 2 August 2017, this quiet and thoughtful intelligence man lost no time in rejecting statements that the Bureau is in turmoil. He also ignored one tweet that urged him to 'clean house'.

Wray defended staffers and declared: "There is no finer institution, no finer people than the men and women who work there and are its beating heart."



FBI senior officials and officers are far from pleased with the "in tatters" and "worse than ever" remarks

response to the president's comments. On Instagram he wrote: 'Three things cannot be long hidden: the Sun; the Moon and the Truth'.

For the record, President Trump's Twitter account can boast a remarkable 44 million followers. He says this allows him to "circumnavigate fake media" and reach around 100 million people using Twitter and various social media sites. Interestingly, the president himself only follows 45 accounts.



Christopher Wray is sworn in as FBI Director

"The FBI I see is tens of thousands of brave men and women working as hard as they can to keep people they will never know safe from harm."

Asked if his comments were a response to the president's harsh words, Wray refused to be drawn, but candidly said: "My experience has been that our reputation is quite good." However, he did concede that agents make mistakes, but added, "processes are in place to hold them accountable."

All of the recent banter stems from the president's belief that elements in the FBI chose to ignore wrong-doings in the investigative probe of his 2016 General Election opponent - Hillary Clinton. This ultimately led to the dismissal of James Comey by Trump.

• 35,000 people are employed by the FBI

Classified: The Insider's Guide to 500 Spy Sites in London

Incorporating highlights and significant moments of over 100 Years of British Secret Service 1909-2015

PLUS 250
ASSOCIATED
LONDON
INTELLIGENCE
SITES

Classified: The Insider's Guide to 500 Spy Sites in London provides visitors to the UK's capital with a unique opportunity to journey to places that are forever embedded in the city's fantastic spynore. Also included are many forgotten sites where spies from around the world have conducted their own secret war with MI5 and MI6. Service headquarters, covert hiding places, secret front companies, agent training locations, mail opening centres, underground venues, safe houses, dead letter drop sites and the darker side of this fascinating 'cloak and dagger' world are explored, including assassination and murder most strange. There's also a splendid candid commentary about the history of Britain's Secret Service from its inception in 1909 to the present day.

This informative work produced by the editorial team of Eye Spy Intelligence Magazine reveals London's enduring liaison with the world of espionage. An illuminated history of secret spy games, tradecraft and treachery hosted by one of the greatest cities in the world... indeed, the spy capital of the world!

- Full colour throughout • 544 pages with complete index • Over 1,900 photographs
- 1,000 specially commissioned images • Large format 210mm x 270mm

THE ULTIMATE SPY SITES TRAVEL GUIDE OF LONDON

UK £22.50
USA \$32.00
WORLD £25.00
PRICE INCLUDES
P&P/AIR MAIL!

To order use form on page 82 or via Internet -
<http://www.eyespyimag.com/500-book.html>

OR TELEPHONE EYE SPY DIRECT: 01756 770199 UK
TOLL FREE: 877 309 9243 NORTH AMERICA

• 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

NEW SERIES

10 TRADECRAFT

COMMUNICATION METHODS

SUITS, TIES AND FLOWERS

From the wearing of flowers in buttonholes on men's suits, to hat types, shoe buckles and umbrellas, clothing and accessories have been used as signs, signals and instructions as covert messages and prompts.

The 'sign' that initiated the exfiltration of MI6 agent Oleg Gordievsky from Moscow in 1985, was a simple Safeway supermarket bag. In this case MI6 told him if he ever thought his life was in peril he should walk down a certain street at a certain time carrying the bag. And then one evening he did. MI6 surveillance officers were watching, and duly organised his escape to Finland.



Iraq's Naji Sabri addresses United Nations... with CIA-supplied suit

Another classic example of 'garment tradecraft' occurred in 2002, when the CIA made contact with Iraq Foreign Minister Naji Sabri - the objective being to source intelligence on Saddam's WMD. The CIA, unsure if Sabri would cooperate, thus delivered a suit to his hotel in New York where he was about to speak at the United Nations. If Sabri was 'onside' he would deliver his speech wearing the suit. And he did - whilst also pocketing a covert \$1 million payment.



Oleg Gordievsky escaped his KGB watchers



THE LIBRARY BOOK

Sadly today, libraries are closing down by the score, but there was once a time before the age of the Internet, when these important places of learning were numerous in towns and cities, and frequented by the masses. They were also utilised fully by those engaged in espionage. Messages and information could be left in specific books and/or exchanged without turning to the spoken word. In virtually all cases, the users were conversant with the target book, or subject, making

selection relatively easy. Similarly, the topic would change regularly, allowing some degree of protection; and to add a layer of additional security, operators would select obscure subjects.

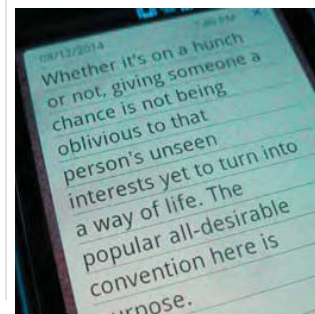
Today, Eye Spy was informed the passing of information, conversation and covert liaison has now switched to another instantly recognisable location. High street gambling outlets dwarf libraries in respect of numbers, and few even glance at the writings on betting slips exchanged between users.

SECRET WRITING

In 1839 playwright and novelist Edward Bulwer-Lytton wrote *'The pen is mightier than the sword'*. Few in the game of espionage would disagree, though often the actions of collectors and distributors of information, be it coded or otherwise, tend to impact sooner or later on the latter.

Secret writing - inconsequential numbers, seemingly nonsensical scribbles and trivial statements have been used by those operat-

ing in the high and dark echelons of government for thousands of years. They continue to be used in the intelligence world today.





Their meaning is often known by just a few - the end user[s]. Adaptations of written information has evolved of course, from one-time pads, prompts - the location of further material or a meeting point, to warnings of imminent danger. Sometimes statements are intended for adversaries - and this involves properly formatted news items published in seemingly credible news reports. In this case, the intention is little more than deception.

Other classic 'time capsules' of secret writing can also be found in this category, such as the use of invisible ink, and in later times bland and meaningless photographs and sketches to depict or impart information.

SIGNS, SCRIBBLES AND MARKERS

In the high intensity days and dangerous period of the Cold War, spies from both the East and West often chose to use unique symbols and seemingly irrelevant markers or objects to communicate. British naval traitor John Vassall is a good example. In 1954, he was recruited by the KGB in Moscow and soon later found himself back in London working for the Admiralty. When

Today of course, spy agencies and certain underworld organisations utilise the Internet. Here authentic messaging, sometimes just a single line, can be hidden in voluminous amounts of information, where only the informed have access or knowledge to its exact location and meaning.

The manner in which secret writing can be further protected is limited only by the imagination of those utilising such tradecraft. But just like any code, once discovered it is vulnerable: there still exists counter-intelligence specialists skilled in the art of deciphering and codebreaking, and today's powerful computer programmes augment such tasks.

he needed to meet his handler, the spy would draw a simple pink circle on a tree or fence near his London flat.

Other odd markers were also used in Britain's capital, such as leaving train tickets attached to lamp posts or a discarded bottle near a bin in a London park. Sometimes even a simple scratch on a wall or the piercing of a milk bottle top

would initiate contact. In Washington, there were even tales of orange peel being left on footpaths. Like before, their meaning would only be known to those engaged in the activity.



John Vassall



DEAD DROPS AND TRANSPORTATION

The use of dead letter drops or dead drops (DD) to pass physical packages has been covered extensively in Eye Spy, yet the utilisation of this tradecraft continues to this day. However, like many elements of information exchange, technology has seen the 'engineering' of the DD evolve.

Today, there are case examples where the genesis of a dead drop begins in the hidden regions of the Internet... or DarkWeb to be more precise. Here operators will source specific information on locations in city streets and woodland (for example) prompting a person to an exact location where an item can be recovered. And the tradecraft is a relatively

secure method unless of course the 'collector' or 'provider' is known to an intelligence adversary who will undoubtedly conduct surveillance.

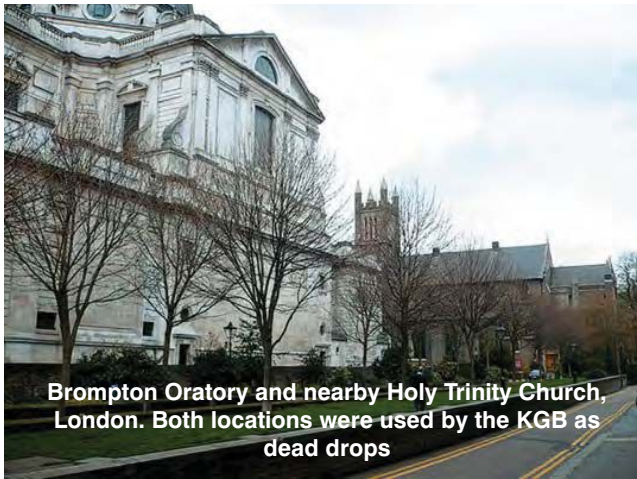
When one thinks of a dead drop, naturally the mind conjures up an image of a hollowed out tree stump, or a location which seems innocuous - beneath a wooden sign post, public toilet, a gap between a brick wall etc. Today, intelligence eyes are also focussed on larger targets, such as ports and the movement of illegal weapons, high-end technology and other materials - many of



KGB spies in Washington reportedly used orange peel as a prompt to a secret location



Weapons bound for ISIS in North Africa recovered by security services in Greece. Inset: The cargo ship Haddad was registered in Bolivia



Brompton Oratory and nearby Holy Trinity Church, London. Both locations were used by the KGB as dead drops



Interior Brompton Oratory. Inset: Behind this pillar KGB operatives would conceal and exchange materials



5000 firearms were concealed in boxes labelled as 'furniture' on the cargo ship Haddad

which are now called 'Freight' in the intelligence world and require shipping or air transportation. All far too big to secret into a tree stump or bury.

Yet the genesis of a journey or covert operation (illegal) to move

such items often begins with a simple communication between supplier and end user, just like users of 'traditional' dead drops. And for those engaged in uncovering such actions, it is just as important to identify all secret aspects of a warehouse or container's use - from assembly to departure and the eventual arrival point. Just as important, the operators of the location, or those renting a facility.

Some aspects of this underworld trade have been compared to dead drop usage.

Dead Drop 'spike'
COURTESY: CIA



FBI officer and KGB spy Robert Hanssen used this bridge as a dead drop

COMMUNICATION OBJECTS

Cannisters, boxes, bolts, rings, watches, tins, bottles, newspapers and virtually any everyday and recognisable item has been used in history and adapted to carry information or project a message or signal. Spylore is littered with case files where those engaged in the art of espionage have opted to use objects that attract little attention and afford much security, from 'worry beads' to Rubik Cubes, the latter being carried as a signal to those attempting contact in 2013 with NSA traitor Edward Snowden. In this case Snowden asked former *Guardian* correspondent Glenn Greenwald, to make his way to a hotel carrying the object before contact was made.

The KGB were ardent users of hollowed-out coins, but the inadvertent discovery of one such coin at a New York address in 1953, dubbed the 'lucky coin', eventually led to the downfall of a spy ring and arrest of a senior spy



Rudolf Abel and an FBI image of the 'lucky coin'

- Rudolf Abel. A young newspaper delivery boy - 'Jimmy' - had asked a couple for change of a dollar bill. He later dropped the nickel which opened revealing microphone film. This prompted the Bureau to launch a major investigation. And of course, Abel was later exchanged for CIA U-2 pilot Gary Powers in 1962.



Edward Snowden, Glenn Greenwald and a Rubik Cube

IDENTITY EXCHANGE

One of the more subtle and dangerous spy activities watched more and more intensely by agencies such as MI5 and the FBI, is the covert placement of individuals from foreign lands into places of learning and high-end technology houses, often with military threads. Once embedded into an organisation or company, information loss is inevitable.

Eye Spy has learned that covert programmes have been initiated by several counter-intelligence

organisations and military bodies to identify individuals who have been 'schooled' by government bodies in countries such as China - ultimately to find work in





overseas companies - preferably government or technology bodies.

And this programme or ruse begins at a very early age; the students are prepared and supported whilst abroad, first entering a university and then securing a position at a defence contract company, for example. Unbeknown to the host nation, they are in fact being readied for a life in espionage.

Often given secure cover and legend, and in many cases, a totally new identity, a role within a defence contract company, will invariably give them access to technology. There follows communication - and the transfer of useful and sometimes highly classified information to a support team or handler.



Little wonder China, for example, continues to baffle intelligence people with their duplication of many Western technologies and military hardware which not only resembles such hardware as aircraft, tanks and shipping, but also utilises the technology which such systems use!

Identity creation or exchange is therefore an obscure, but major stepping stone in the information and communication elements of Intelligence. And once a person is established and a corridor of contact enabled, the operation is very difficult to detect and defeat.

BRUSH PASS AND EXCHANGES

If ever a tradecraft has survived the passage of time and avoided the pit falls (and advantages) of the Internet, then it must surely be the 'legendary' Brush Pass. The passing of information and items utilising environment, objects and of course, the skill of participants.



In basic terms this is simply agent contact using sleight-of-hand to exchange materials. This can be performed in plain sight, in busy locations such as a crowded street, or even in remote places. It often involves two people simply walking towards each other and covertly handing over a package. Performed in a microsecond, the exchange is almost invisible to the naked eye. Other variants exist, of course, such as sitting at a park bench and dropping an item into a bag; or indeed, departing with the other person's bag. In some



The 'bag switch' - easily performed and usually involves identical bags/cases

known cases, MI5 surveilled KGB spies actually switching bags in London parks.

Members of the Russian SVR spy ring which operated for over a decade on the eastern seaboard of the USA, before being deported in 2010, also used the tradecraft - an indication that even today the 'art' is considered valuable.

Unless under surveillance by skilled counter-intelligence people, the bag switch and brush pass will not attract attention - in virtually any environment.



Russian SVR spies caught on a covert FBI surveillance camera perform a 'brush pass' and 'bag switch'

ORDINARY PEOPLE

Like it or not, and despite a plethora of denials from those who run and oversee spy agencies, information transfer is often performed using 'ordinary people'.

A 'person of interest' who exits or enters a foreign country will inevitably be required to impart exact details of their journey and the reason for the excursion, be it a holiday or business trip. Questions will also be raised as to his or her's address or hotel and the length of their stay.



At airports and sea ports bag searches are a norm, and none more so when the individual is on a watch list, be they suspected of working for an intelligence agency, criminal gang or simply a character acting suspiciously. If that person is indeed on an assignment, then in many cases an intelligence agency may opt to use a decoy to carry information, and in some cases, this involves an innocent person whose luggage has been accessed.

Such events are rare, but secret-ing information or a piece of technology into a third party's



luggage is possible using airport associates (baggage handlers for example), or even at home, prior to their journey. Thereafter recovery of the item and delivery must take place - and two words come to mind 'lost luggage'.

The art is uncommon and dangerous, especially to the innocent party. However, when the stakes are high, some intelligence



services (and underworld organisations), will decide that the risks outweigh other options.

INFORMATION REQUESTS

One masterspy used a simple method to secure secrets... he requested them. Often intelligence, or a gateway to intelligence, can be acquired by non-provocative actions away from the prying eyes of spycatchers.

Frederick Duquesne was head of a WWII spying operation in the United States. He would scan military-related features in the American media, especially the *New York Times* for stories which he believed would be useful to Germany.

By 1939, he had already passed material on new bombers, flying instruments, range-finders and all manner of military hardware, including blueprints... all available through contracting companies. He simply wrote for them. And his eyes lit-up again when the NYT

claimed the US Army's Chemical Warfare Service was developing a 'mysterious new gas mask'.

Duquesne realised this could be a gateway to clues on a range of new poison gases being developed by the same organisation. Access to the top secret Aberdeen Proving Ground where tests were being conducted was impossible, so he created a ruse by posing as a 'well-known responsible and reputable writer and lecturer'. Duquesne wrote to the US Army requesting information: *'Don't be concerned if the information is confidential, because it will be in the hands of a good, patriotic citizen'*.



ALL PRICES INCLUDE POSTAGE (AIR) AND PACKING

UNDERCOVER BOOK RELEASES

THE HITLER CONSPIRATOR: The Story of Kurt Plettenberg's Valkyrie Plot to Kill the Führer

Eberhard Schmidt
Frontline Books

Kurt Baron von Plettenberg (right) was the descendant of a Westphalian aristocratic family, and a soldier in both world wars. The expectations, which he initially had, along with many of his fellow conspirators of the 20 July 1944 plot to kill Hitler evaporate, when he recognises the true nature of the regime. When he accepted the office as general agent of the former Prussian royal house of the

Hohenzollerns in 1942, Plettenberg already belonged to the inner circle of the resistance planning Operation Valkyrie. After the assassination attempt, however, he was not immediately identified as one of the conspirators. Yet only a few weeks before the end of the war,

Plettenberg was finally denounced and arrested.

This biography shows for the first time how Kurt von Plettenberg,



who belonged to the inner circle of conspirators and assassins, found a way to prevail during those difficult times and how significantly he influenced the resistance. Hardback 256pp

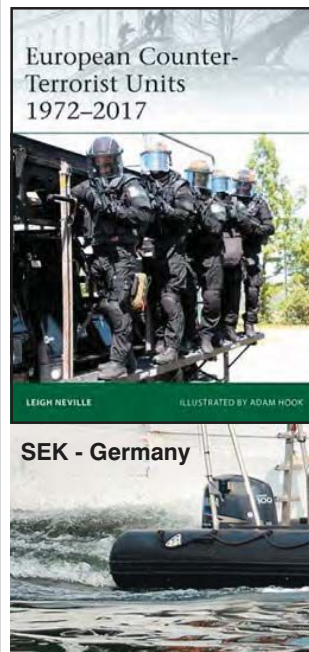
Available from Eye Spy Ref: ES/1690
UK £22.50 USA \$30.00 ROW £24.50

EUROPEAN COUNTER- TERRORIST UNITS 1972-2017

Leigh Neville and Adam Hook
Osprey Publishing

The Munich Olympics massacre in 1972 was a shock awakening to the public of international terrorism. In the decades since, European

countries have faced a wide range of threats from foreign and home-grown terrorists, to the more recent worldwide jihadists of ISIS. The threats they pose are widespread from aircraft hi-jacking and political assassinations to urban warfare against security forces, and murderous attacks on civilian crowd targets, forcing governments to invest ever-greater efforts in countering these threats.





1941. Nazi spy Frederick Duquesne is interviewed by FBI officer Harry Sawyer

Amazingly, the letter was received and a few days later a series of documents providing intimate details of the new gas mask arrived at his New York apartment. These were duly forwarded to his spymasters in Berlin and allowed German scientists a unique insight into America's covert WMD industry.

And this simple 'request' communication tradecraft exists today, utilising bogus front companies and individuals who are little more than 'players' in the great game.



Yamam - Israeli counter-terrorist unit

This excellent book traces the evolution of police (and associated military) counter-terrorist forces across Europe over the past 45 years. Using specially commissioned artwork and contemporary photographs, it details their organisation, missions, specialist equipment, and growing cross-border cooperation. Softback 64pp ➤

Available from Eye Spy Ref: ES/1691
UK £10.99 USA \$18.00 ROW £11.99



THE WORLD OF INTELLIGENCE CRESTS

SUPERB QUALITY POSTERS - A UNIQUE GIFT

- luxury 170gm weight paper • full colour
- giant A2 size (23.5 x 16.5 inches)



EACH POSTER -
REF: ICP1, ICP2 & ICP3 -
UK: £6.50 USA: \$14.00
EUROPE/WORLDWIDE: £8.50



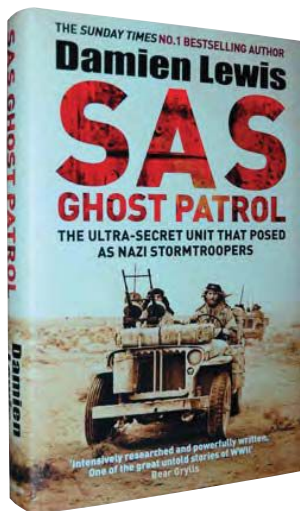
**Or as a Combination Set - REF: IC123 - UK: £16.00
USA: \$30.00 EUROPE/WORLDWIDE £22.00**

PRICE INCLUDES P & P AND ALL SHIPPING COSTS. OVERSEAS ORDERS ARE DESPATCHED AIR MAIL. PLEASE USE FORM ON PAGE 82 OR ORDER ON-LINE - www.eyespyimag.com

SAS GHOST PATROL: The Ultra-Secret Unit That Posed As Nazi Stormtroopers

Damien Lewis
Quercus

Lewis's *SAS Ghost Patrol* is the explosive true story of the day in 1942 when the SAS donned Nazi uniforms to perpetrate the most audacious and daring mission of the war. Beyond top secret, deniable in the extreme (and of course enjoying Churchill's enthusiastic blessing), this is one of the most remarkable stories of wartime lawlessness, eccentricity and raw courage in the face of impossible odds - a thoroughly British undertaking.



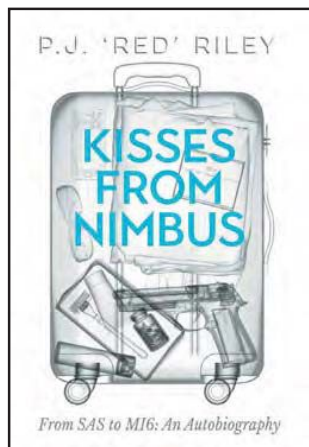
What unfolded - the longest mission ever undertaken by Allied Special Forces - was an epic of daring, courage, tragedy and survival that remains unrivalled to this day, and which rightly became a foundation stone of Special Forces legend. Written with Lewis's signature authenticity and dramatic verve, the book is peopled by a cast of the utterly maverick and the extraordinary. In its quirky eccentricities and outrageous rule-breaking, this is a story that only the British could have authored, and with such panache and aplomb! Hardback 352pp

Available from Eye Spy Ref: ES/1692
UK £22.50 USA \$34.00 ROW £24.00

KISSES FROM NIMBUS: From SAS to MI6 - An Autobiography

P. J. Red Riley
Clink Street Publishing

Shot at, bombed, imprisoned and arrested for murder. Captain P. J. 'Red' Riley is a former ex-SAS soldier who served for eighteen years as an MI6 agent.



Riley escaped internment in Chile during the Falklands War whilst engaged in an audacious top-secret attempt to attack the Argentinian mainland. He was imprisoned in the darkness of the Sierra Leone jungle, and withstood heavy fire in war-torn Beirut and Syria.

In 2015, he was arrested for murder but all charges were later dropped.

In this absorbing memoir, Riley reveals the brutal realities of his service, and the truth behind the newspaper headlines featuring some of the most significant events in recent British history. His account provides informative new evidence on the Iraq war, what Tony Blair really knew about Saddam Hussain's weapons of mass destruction before the allied invasion, and questions the British Government's alleged involvement in the death of Princess Diana.

Controversial, chaotic, darkly humorous and at times heart-wrenchingly sad, *Kisses From Nimbus* charts the harrowing real-life experiences of a soldier and self-confessed spy in the name of Queen and country. Hardback 216pp

Available from Eye Spy Ref: ES/1693
UK £17.50 USA \$25.00 ROW £19.00

TROTSKY'S FAVOURITE SPY: The Life of George Alexander Hill

Peter Day
Biteback Publishing

Una Kroll was 11-years-old when she met her father for the first time, and was distraught when, at that same meeting, he told her he would not be coming home... he had another life. To explain away the absence of her mysterious father, the young Una had always told her classmates that he was an aviator and explorer who

© JUDY MADDOCK



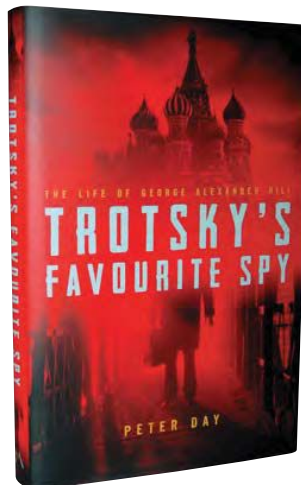
had gone missing in the desert. This was far less extraordinary than the truth, which she discovered years later.



Una's father was George Hill, a British spy who befriended Leon Trotsky (left) during the Russian Revolution, smuggled the Romanian

crown jewels out of the Soviet Union and was involved in a doomed attempt to rescue the Tsar's family. During WWII, he was the link between Churchill's Special Operations Executive (SOE) and Stalin's secret service. He was a man capable of great bravery, but little compassion.

In this gripping biography, acclaimed writer and journalist Peter Day shines a light on the shadowy world of twentieth-century espionage. It was the age of swashbuckling secret agents,



swordsticks and clandestine assignments, and it is vividly brought to life through the story of George Hill, one of Britain's most remarkable spies. Hardback 304pp

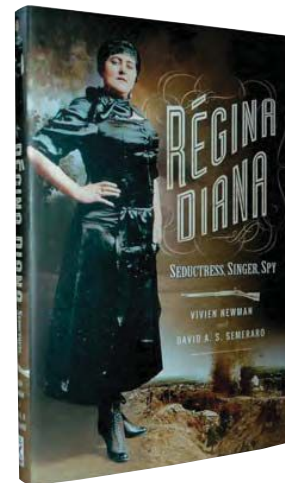
Available from Eye Spy Ref: ES/1694
UK £22.50 USA \$30.00 ROW £24.50

REGINA DIANA: Seductress, Singer, Spy

Vivien Newman, David Semeraro
Pen & Sword History

The untold story of Regina Diana tells of the rebellious daughter of working-class French-Italian parents from a run-down area of Geneva who, trained by the most ruthless spymaster of them all, Elisabeth Schragmuller (A.k.a. Fraulein Doktor), became a much-adored French cafe-concert singer, a discreet and highly-prized prostitute plying her trade, and a successful German WWI spy.

Regina's spy operations were full of intrigue: a network spanning four countries based in the city of Marseille, with her performing abilities and sexual charms allowing her to lure men from privates to generals into giving her vital information.



This book is not just about Regina, but also explodes the much-vaunted myth of Swiss neutrality. Switzerland, a nest of spies, was riven between support for Germany and France; in an extraordinary penetration of the upper echelons of Swiss society, the Swiss Army Commander-in-Chief was married to former German Chancellor Otto von Bismark's daughter. Yet exhuming Regina from her unmarked grave involved a tantalising journey - getting past her disavowal by both

France and Switzerland, unravelling the truth behind a three-line report about a pretty Swiss singer's execution and overcoming the obfuscation of French military archivists. Even her execution was fittingly exceptional. So determined were the French authorities that she should die, her firing squad numbered not the usual twelve, but twenty-five smoking rifles. Hardback 192pp

Available from Eye Spy Ref: ES/1695
UK £22.50 USA \$30.00 ROW £24.50

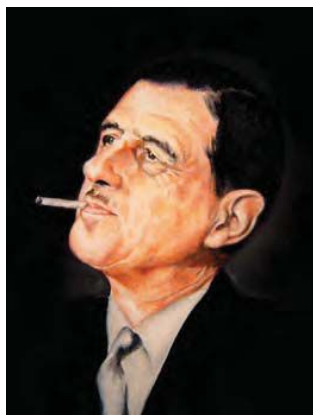
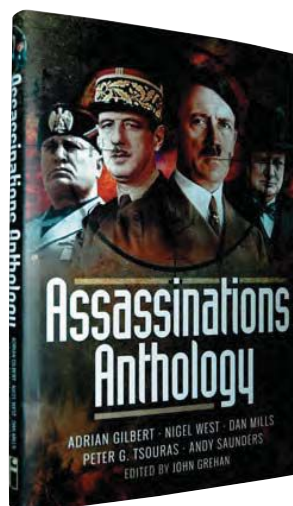
ASSASSINATIONS ANTHOLOGY: Plots and murders that would have changed the course of WWII

Edited by John Grehan
Frontline Books

The infamous Valkyrie assassination attempt on Adolf Hitler on 20 July 1944 failed to kill the German Führer. It was a very close call, and has led to endless speculation about what might have happened if the briefcase bomb plot had succeeded.

Equally intriguing is the failed assassination attempt on General de Gaulle on British soil. Who, one wonders, was behind that scheme, and how would Anglo-French relations have developed if he had been killed? If the aircraft he was to fly on set off just a few minutes earlier would it have crashed to the ground?

In *Assassinations Anthology* a number of well-known authors and historians have looked at past events where key individuals were involved in either attempts on their lives, or strange incidents occurred which, had they led to their deaths,



Portrait of Charles de Gaulle

might have radically affected the outcome of the war. Events surrounding Stalin and Jan Smuts are investigated, as well as the peculiar circumstances relating to the theft of a valuable Gainsborough painting. Just how great a role did the Government's Chief Whip, David Margesson, play in persuading the MPs to accept the unpopular Winston Churchill as Prime Minister, and what would have happened if Margesson had been killed when the Gainsborough disappeared?

Grounded in actual events, the various scenarios portrayed in this collection examine the likely chain of events that would have followed if the assassination attempts had succeeded. A few inches, a few minutes that was all the difference between life and death, and between the past that we know and one that we can only imagine. Hardback 188pp

Available from Eye Spy Ref: ES/1696
UK £22.50 USA \$30.00 ROW £24.50

ALASTAIR DENNISTON: Code-breaking From Room 40 to Berkeley Street and the Birth of GCHQ

Joel Greenberg
Frontline Books

In 1914 Alastair Denniston, who had been teaching French and German at Osborne Royal Navy College, was one of the first recruits into the Admiralty's fledgling codebreaking section which became known as Room 40. There a team drawn from a wide range of



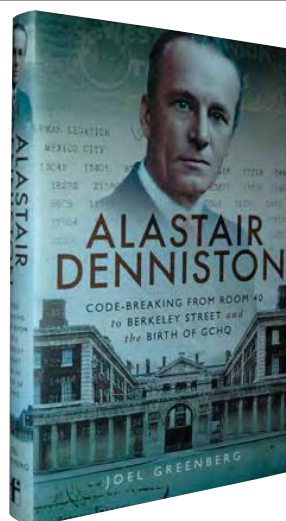
Alastair Denniston

professions successfully decrypted intercepted German communications

© GCHQ/CROWN COPYRIGHT



2017. The Denniston family at GCHQ with author Joel Greenberg (far left)



throughout the First World War. After the Armistice, Room 40 was merged with the British Army's equivalent section MI1 to form the Government Code and Cypher School (GC&CS).

Initially based in London, from August 1939 GC&CS was largely located at Bletchley Park, with Alastair Denniston as its Operational Director. Denniston was moved in 1942 from military to civilian intelligence at Berkeley Street, London. Small at first, as Enigma traffic diminished towards the end of the Second World War, diplomatic and commercial codebreaking became of increasing importance and a vital part of Britain's signal intelligence effort. GC&CS was renamed the Government Communications Headquarters (GCHQ) in June 1946.

Denniston's death in 1961 was largely ignored by major newspapers and the very British intelligence organisation that was his legacy - GCHQ. Hardback 308pp

Available from Eye Spy Ref: ES/1697
UK £27.50 USA \$38.00 ROW £29.50

NUCLEAR WEAPONS MANUAL: (Operations Manual)

David Baker
Haynes Publishing

Much misinformation has been published by those who support, as well as those who are against, the continued deployment of nuclear weapons as instruments of deterrence. The book provides a descriptive overview on what they are, how they are categorised, how they would be sent to their targets and how their design and potential application has changed.

This book incorporates a balance of cutaway diagrams, images of hardware and test equipment, facilities and delivery systems, and traces the evolution of nuclear weapons over the past 70 years, with the emphasis on strategic nuclear delivery systems today.

An excellent guide expressed in a dispassionate and factual manner - information which many people find hard or impossible to obtain. Large Hardback 192pp

Available from Eye Spy Ref: ES/1698
UK £20.00 USA \$30.00 ROW £22.50



THE ADVENTURER

US Navy Captain Leonard LeSchack **CIA ANALYST, AUTHOR AND SPY**



One of life's great intelligence adventurers and friend of Eye Spy, Captain Leonard LeSchack, sadly passed away shortly before Christmas 2017

Born in Freeport, New York in 1935, LeSchack, was encouraged to live a life of adventure. His father was a lawyer and his mother a history teacher and they read to him daily about explorers, adventurers and inventors. By 1957, Len was asked to join the US Antarctic Expedition as an assistant seismologist. Based on the work he performed in the Antarctic, he had a mountain range named after him - Mount LeSchack - in the Wisconsin Range, Horlick Mountains.

Early on, he noticed a common denominator about all his favourite explorers: they were

either commissioned by the Government or had military training. Since the US Navy handled most of the logistics, he got to know the Navy officers and men, resulting in the Navy's senior commander in the Antarctic agreeing to recommend him for Navy Officer Candidate School after returning to the United States.

Eye Spy readers are familiar with his work on one of the most daring and original Cold War military operations - Project Coldfeet* (1962). It was his brainchild to investigate a recently abandoned Soviet drift station to determine if the Russians had the capability to track US

By Susan Lucas



'Seven Days in the Arctic'

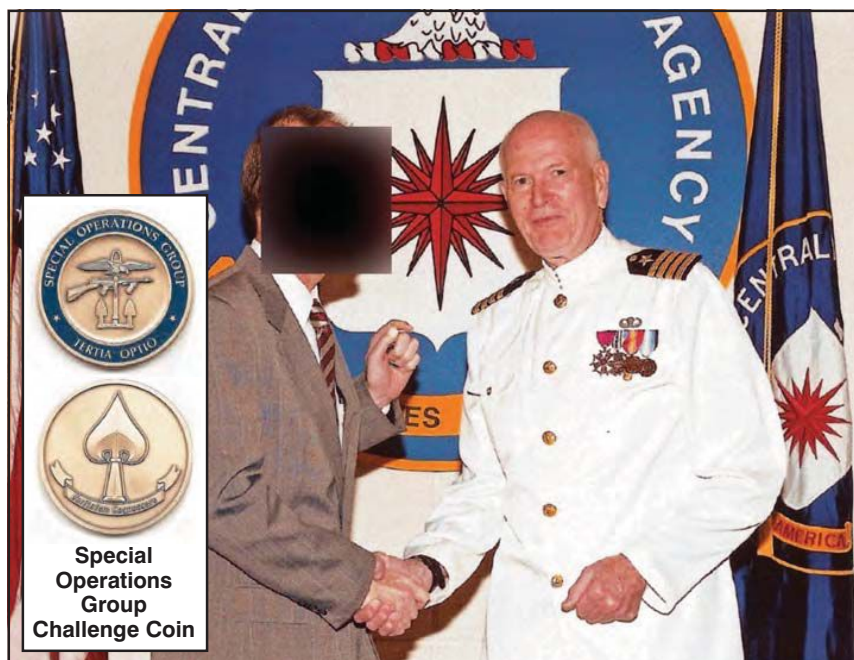
submarines. The CIA provided the aircraft with a unique Skyhook Aero-retrieval system developed by Robert Fulton; the Navy and USAF were all involved in both the dropping and extraction of both Leonard and one other participant. Captain LeSchack had exactly what he wanted... adventure!

Operation Coldfeet was a definite success, and LeSchack received the Legion of Merit for

Leonard LeSchack (centre) with intelligence associates at CIA headquarters, Langley, Virginia



COURTESY CIA



2008. CIA headquarters, Langley, Virginia. Leonard LeSchack receives his Special Operations Group Challenge Coin from a senior CIA official

Project Coldfeet. A painting of the Project Coldfeet mission called 'Seven Days in the Arctic' by artist Keith Woodcock proudly hangs in the CIA Museum.

Thereafter numerous posts saw LeSchack travel extensively and he performed various US Government contracts. The Navy eventually called him back to active duty to run the Cuban-Haitian Refugee Center in Puerto Rico, then ordered him to the US Naval Station at Panama Canal where he became that command's intelligence officer.

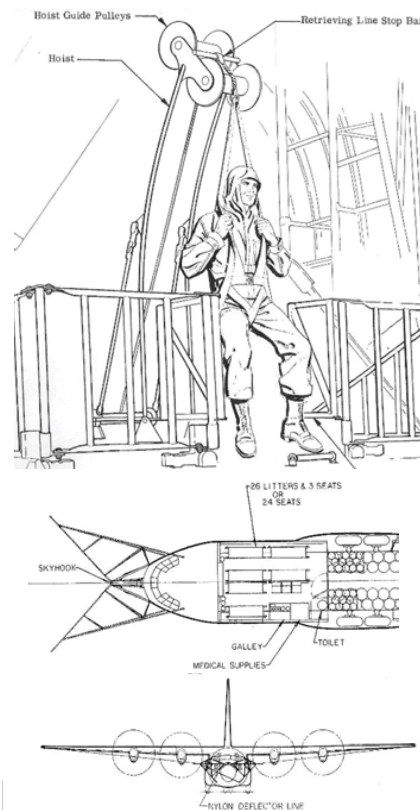
After his release from active duty and his move into private research, the military invited LeSchack to establish a Naval Reserve Intelligence Unit to support the then-recently established US Forces Caribbean Command in Key West. He became its first commanding officer and served as Deputy Chief of



Fulton Skyhook in operation

Intelligence for that command. Other significant private contracting tasks followed.

Captain LeSchack co-authored *Project Coldfeet* with William M. Leary and published his memoirs four years ago - *He Heard a Different Drummer: The Cold War Memoirs of a Scientist, Explorer, Naval Officer and Spy*. He continued to be active in writing and editing with myself (a close friend and co-author), and he presented lectures on our need for



Fulton Skyhook deployed on a C-130

greater Arctic security to counter Russian activity in that region.

As per his wishes, Leonard was buried in Arlington Military Cemetery in early 2018. He considered it an honour and privilege to be amongst the service personnel there.

- Susan Lucas has written an indepth overview of the life of Captain Leonard LeSchack available on Eye Spy's website.

LINKS: www.eyespyimag.com

***Operation Coldfeet: The Covert Soviet Ice Station Mission - Eye Spy 80 and 81**



B-17G 'Shady Lady' as she appears today in Evergreen Aerospace Museum. The aircraft was just one of a small number to have carried the Fulton surface-to-air recovery system

© EVERGREEN AVIATION & SPACE MUSEUM, PROVIDED BY MR STEWART BAILEY, CURATOR

ADVENTURE IN TIME COMMUNICATION & ESPIONAGE

Continued from page 31

Just as damaging was the fact that adversaries in Russia, China, Iran, North Korea and elsewhere, now had intimate details of how US and UK intelligence services collected information, methods, future ambitions and the agencies dedicated to this endeavour.

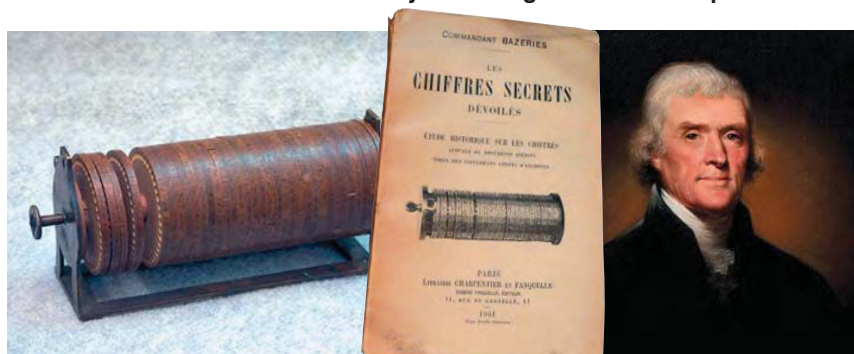
PENETRATION

In Intelligence work, layers of security to protect information and communications are usually many and require a high degree of planning. More thought is given to those sectors identified as being of particular use to an adversary. They are updated and monitored frequently to protect against penetration.

Yet history has shown that any communication breach and lack of security in a government department can have dreadful consequences. A world away from Snowden's activity, take for example the classic WWII case of Hans Thomsen, a career diplomatic and Charge d'Affairs at the German Embassy in Washington. As early as September 1939, he had managed to access secrets held at the US State Department via a friend who operated in the code room. The espionage was easy because security was dreadful and the methods used to protect state secrets had not been changed for three decades, despite a number of highly sensitive codebooks and projections disappearing over the years. Amongst the material stolen by Thomsen, was



Information secured in the great game will almost invariably influence and determine decisions made by those in government and power



The Jefferson Disk, *Les Chiffres Secrets Devoiles* (The Secret Numbers Unveiled) by Etienne Bazeries and Thomas Jefferson

a cryptograph system used by the USA to communicate with all its overseas embassies and outposts. Indeed, it transpired the system was actually first conceived 150 years earlier by Thomas Jefferson, the first US Secretary of State and thereafter properly developed by Etienne Bazeries. Called the Jefferson Disk (also known as the Bazeries Cylinder) the system had never been updated or its mechanism altered. Now Hitler had access to so many secrets concerning America's (and other nations - Spain and Portugal, for example) wishes to remain neutral. And for the record, the German operation continued for an astonishing 18 months.

Fast forward to 2017, and still government departments and major businesses continue to use aged security systems and procedures. Numerous warnings have recently been issued about antiquated (outdated) cyber security defences and lax monitoring systems.

HUMINT AND COMMUNICATIONS

Questions have recently been asked of the CIA: why Langley failed to warn of North Korea's rapid advance towards securing a nuclear device? One explanation is the lack of human intelligence (HUMINT). North Korea could be likened to Andrew Parker's "digital oasis" in that all Western Intelligence services have found operating in North Korea difficult. And for those who question why spy satellites have not been used to collect photo intelligence, the short answer is much of NK's quest to build weaponry has been moved to underground premises. Whilst road and building infrastructure can provide clues, infiltrating agents inside the country has been difficult - and passing qualified information to friendly agents even more problematic.

Whilst official confirmation has yet to appear, intelligence sources acknowledge agents and contact people have been eliminated by North Korea. A likely victim of this purge is North Korean leader Kim Jong-un's half brother Kim Jong-nam who was assassinated in Malaysia by NK agents in February 2017 (See Eye Spy



Hans Thomsen
Charge d'Affairs
(front right) at a
diplomatic function
and inset



The controversial Sinchon Museum of American War Atrocities



109). He is thought to have had contact with the CIA. Similarly, the South Korean media report that anyone perceived vulnerable to such liaisons or thought to be working for an external Western-friendly body (spying), has been executed, including NK Party members.

Propaganda too has played its part and citizens are continually warned of [US contested] American 'atrocities' committed against its people (Korean War). Indeed, to enhance further this atmosphere of mistrust, in 2015 North Korea rebuilt and expanded its Sinchon Museum of American War Atrocities. Here visitors can find all manner of gruesome exhibits. All of this is intended as a barrier against Western penetration and intelligence collection. Yet despite this, several intel-related programmes have been enabled, including some radio-based. The objective here is one of influence by *audible content*. And there is evidence it is working, with some intelligence sources admitting a number of key defections have already occurred.

SUMMARY

For those who work in communications' security, the task of protecting information is ever changing. New procedures and tighter regulations has also impacted on the activities and tradecraft of those tasked with stealing information. But despite warnings aplenty, there is genuine concern that people, even



those who hold senior positions, have become blasé about information exchange. From experienced businessmen and women who ignore warnings about WiFi interception, to presidential candidates such as Hillary Clinton, whose lack of prowess when it comes to sending and receiving e-mails stunned the world, warnings are still being ignored. And for the record, many in the CIA, NSA and FBI remain concerned about President Trump's continued use of Twitter to communicate.

The same lack of thought often rolls down to those playing the great game, from cell phone usage and calls (ask the CIA unit involved in the abduction of al-Qaida suspect and Milan Imam Abu Omar in 2003), to e-mails and even vehicle GPS usage (maps, locators etc.). All leave digital footprints.

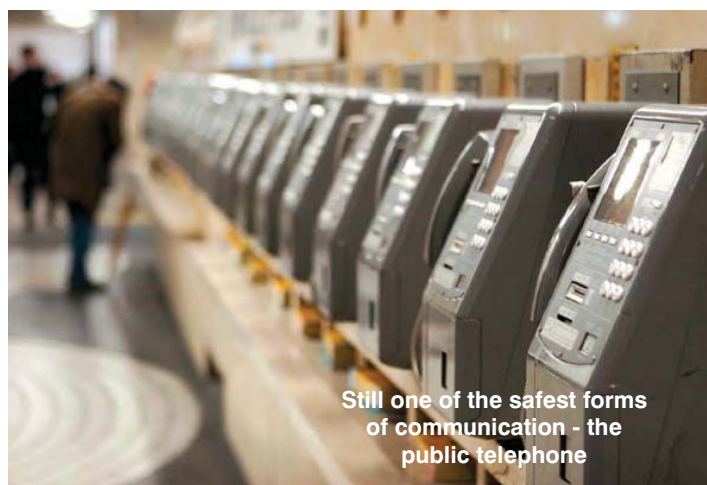
The world of communication can be a very dangerous theatre with actors and spies seeking advantages from the comfort of their

office or home. It is especially problematic for those whose livelihood and operational status (including spies) depends on instant liaison. In the 21st century, people demand immediate and instant communication, and often become frustrated when this is not possible. However, in the intelligence world some experts now recognise that it is occasionally best to resort to old and trusted methods, be it an actual face-to-face conversation in a secure location, or the sending of a letter protected by 'layers' of secret coded meaning. Or indeed, using a public telephone box... if you can find one.

New methods of electronic espionage are being developed every day; the loss of secrets, vital and personal information and embarrassing messaging often lead to compromise.

Despite the development and evolution of powerful interception and communication agencies such as NSA and GCHQ, high impact counter-intelligence services like MI5 and the FBI, this has not stopped of all manner of electronic private companies, individuals, underworld entities and foreign spy agencies intent on mischief operating in plain sight.

The gateway to secrets has changed little since the Greeks first lit their fires thousands of years ago... communication. Understanding and proper use of this tradecraft will always provide an advantage.



Still one of the safest forms of communication - the public telephone

CHRISTINE KEELER



Continued from Page 55

"She wasn't a spy, but was asked to pick-up tittle tattle from her 'clients' and in bustling clubs of London where officers from both sides of the Cold War mixed. Information like this has a price tag. Keeler knew the likes of MI5 head Sir Roger Hollis, where he socialised and his friends. Plus other spies, including double

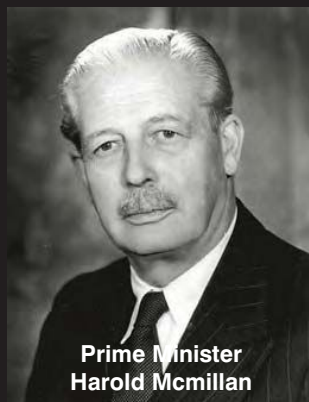
agent and KGB spy Anthony Blunt. It was that sort of world... where spies, glitz, wine, dine and London nightlife merged to form a very dangerous arena. But there were trap doors everywhere and it was inevitable she would eventually fall into one... as did Ward, Profumo and others."

Indeed, in later years Keeler herself acknowledged she had secrets to hide. "I knew I was passing on information but over the years I have always told myself it was just papers... it was not," she said. "Had I been more aware and understood... I would not do anything to harm my country." However, she failed to mention that just before the scandal broke, she tried to sell her story to a newspaper. This is an indication that Keeler was fully aware of the importance of the case.

Keeler says she was "recruited by a very clever man." But well over five decades later, intelligence aficionados still debate which agency that recruiter chose to serve. The answer may still be found in documents MI5 and MI6 refused to release in 2014 regarding the Profumo Affair. The Services insisted that information still relevant to national security of today is contained within, despite it being 50-years-old. And whilst low-key information on the likes of Gisela and Profumo may raise the eyebrow of the odd intelligence



John Profumo



Prime Minister Harold Mcmillan

historian, something of far more significance may still surface.

Christine Margaret Keeler - 22 February 1942 - 4 December 2017

• A new BBC drama on the Profumo Affair is set to air in late 2018.

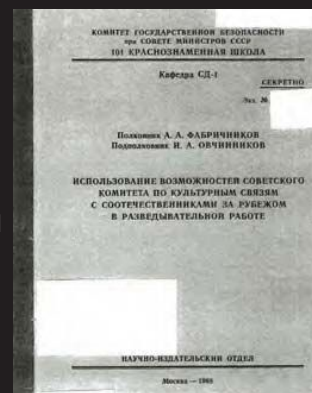
LAST WORD

KGB TRADecraft MANUALS SURFACE

Three KGB tradecraft and teaching files have surfaced in the United States* - reportedly secured from a European-based intelligence agency. One of the manuals dates from around the time of the collapse of Communism and is allegedly still used by Russian Intelligence as a 'teaching tool' for agents and handlers. Their content ranges from agent insertion (diplomatic cover) to preferred meeting locations (theatres, museums etc.) and even how to use disguises. One line reads: 'You will have opportunities to contact foreigners when situations arise, for example, violation of rules, road accidents... agents can be placed in trains and hotels to make approaches'.

The documents, written in Russian, are titled: *Part 1: The KGB Manual for Recruiting Spies; Part 2: The KGB Playbook for Infiltrating the Middle East; Part 3: The KGB Playbook for Turning Agents [People] Worldwide Into Agents.*

*Secured and first published by the *Daily Beast*, it's likely the material has been in the hands of UK and US Intelligence for decades - from defectors and recovered archives following the fall of the Berlin Wall.



OFFICIAL EYE SPY ORDER FORM 2018

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) _____



UNITED KINGDOM EUROPE REST OF WORLD

Eye Spy Intelligence Magazine,
P.O. Box 10, Skipton, Leeds City Region,
BD23 5US, United Kingdom
Or Telephone: 01756 770199 (UK) standard rates

UNITED STATES OF AMERICA CANADA

Eye Spy Intelligence 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

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



Peter Matthews
historical
intelligence



Kevin Coleman
cyber
consultant



Peter Jenkins
surveillance
consultant



Mark Birdsell
managing
editor



Lynn Hodgson
canadian
editor



Paul Beaumont
communications
consultant



Danny King
security
consultant



Kerop Gourdkian
associate
editor



Nick Fielding
senior
consultant



Mike Finn
security
consultant



D. Anne Kohl
associate
editor



Michael Smith
associate
editor



Rusty Firmin
security
consultant



John Nomikos
greece/balkans
editor



Christopher
Eger
naval consultant



Spiros Koptas
associate
editor



Glenmore
Trenear-Harvey
associate editor



Roger Howard
associate
editor



Hala Al-Ayoubi
tradecraft
consultant



John-Hughes
Wilson
consultant



Perin Bhatt
security
consultant

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	£34.00
canada	C\$60.00
australia/middle east/asia/africa	£34.00

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 114

HUMINT

The importance of Human Intelligence has never been greater - as media technology platforms continue to create bogus news stories and distort factual information



EYE SPY INVESTIGATES

AVAILABLE MID-MARCH 2018



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

EYE SPY

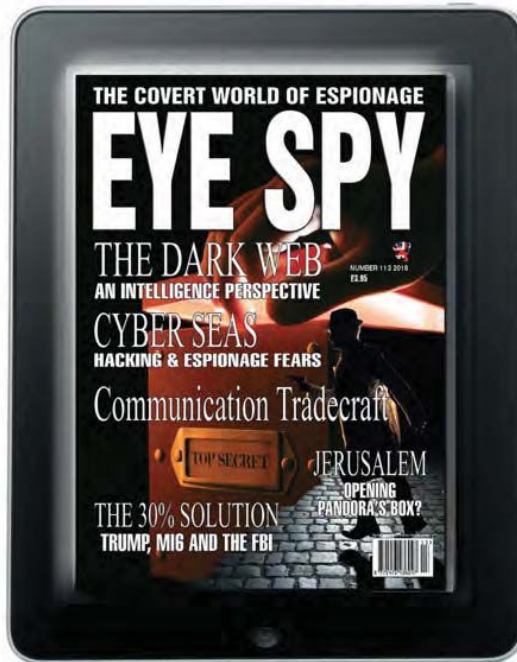
INTELLIGENCE MAGAZINE

DIGITAL EDITION AND FREE APP

THE WORLD'S ONLY NEWSSTAND MAGAZINE DEDICATED TO ESPIONAGE AND INTELLIGENCE IS ALSO AVAILABLE IN ELECTRONIC FORMAT

Documentaries, films, special reports and features, background intelligence, interviews, special links, photo galleries, intelligence documents, slide shows and a plethora of inter-active media

• SUPERB QUALITY • CRYSTAL CLEAR • EASY TO USE



FREE! 118 PAGE APP AVAILABLE FROM

EYE SPY

INTELLIGENCE MAGAZINE

MagazineCloner

pocketmags.com

THE COVERT WORLD OF ESPIONAGE
www.eyespymag.com

Intelligence • secret services • espionage • true mysteries

