

THE COVERT WORLD OF ESPIONAGE

EYE SPY

SPIES TARGET
North Korea

CIA UAV

Covert Kill Programme

CRYPTOCURRENCIES

Primary Tool of Espionage

bitcoin
CRYPTOCURRENCY

ISIS STRIKES IN EUROPE
LONDON AND BARCELONA



NUMBER 111 2017



A-Z

The Language
of Spies



£3.95

Printed and Published in Great Britain



11 >



THE PARK BENCH PLOTTERS

8 Russian-controlled spies alleged attempt to assassinate Montenegro Prime Minister

SPY GAMES



20

CIA UAV Kinetic Kill Programme - Commander Identified

CRYPTOCURRENCIES A PRIMARY TOOL OF ESPIONAGE

25



UKRAINE-NK SPY STING



31



44



COMMUNICATIONS & ESPIONAGE



GHOSTS

ISIS STRIKES IN EUROPE

12 & 78

LONDON • BARCELONA

Another collection of unusual, but authentic terms and phrases used by those who work in intelligence, espionage and security

54

A-Z The Language of Spies

EYE SPY 111



VOLUME XIV NUMBER SEVEN 2017 (ISSUE 111)
ISSN 1364 8446 publication date: OCTOBER 2017
FRONT COVER MAIN IMAGE: TALISMAN INTEL LIBRARY



MAJOR CONTENT GUIDE

- 6 TALON - TAV COUNTER-MEASURES**
New Scotland Yard unveil new terrorist attack vehicle counter-measures following spate of attacks in Europe and elsewhere
- 11 RUSSIAN 'SPY HUB' CLOSED**
US Government closes Russian consulate as 'tit-for-tat' diplomatic manoeuvres continue between two countries
- 20 SPY GAMES**
CIA and FBI point accusing finger at *New York Times* as key Langley operator in Middle East is identified by newspaper
- 23 TURING LETTERS REVEAL DISLIKE OF USA**
A batch of previously unseen letters written by Britain's most famous WWII codebreaker reveal his dislike for the country that afforded so much help to him and colleagues
- 25 CRYPTOCURRENCIES**
A revealing investigative feature focussing on the importance of this new form of money and its use by those in the spying game and underworld
- 29 BREXIT, SPIES AND THE POKER GAME**
European intel watchers accuse Britain of using its powerful spy agencies as leverage in the Brexit negotiations
- 37 POINT OF NO RETURN?**
New North Korea missile launch and atomic capabilities raise further the prospect of conflict in the Far East theatre
- 41 KASPERSKY LABS AND SPY LIAISONS**
US intelligence and government bodies asked to remove Kaspersky software protection from computer systems, as spy fears prompt array of new regulations and countermeasures
- 49 ISIS INTELLIGENCE FOCUS**
An examination of the latest Alliance operations against the terror group as further atrocities continue outside the Middle East theatres carried out by ISIS supporters
- 54 A-Z LANGUAGE OF SPIES**
Eye Spy once again delves into its huge archive of spy terminology created and used by those operating in intelligence and espionage
- 59 FAR BEYOND REASONABLE DOUBT**
United Nations investigators provide powerful evidence Syrian forces used WMD on civilian targets
- 62 THE MYSTERIOUS RUSSIAN BUZZER**
Eye Spy reveals the truth behind an unknown Russian signal which has captured the imagination of conspiracy theorists
- 66 LIFE INSIDE THE LONDON CAGE**
A special feature by intelligence historian Helen Fry examining a controversial WWII London location to 'extract' information from German prisoners of war
- 71 SPY CUBA: US DIPLOMATS TARGETED**
An unidentified sonic 'weapon' appears to have been used against American diplomatic staff on the island of Cuba

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

"Kaspersky Labs would never help any government in the world perform espionage or cyber offensive efforts..."

Eugene Kaspersky on allegations of Russian intelligence Liaisons



FIRST WORD

USING TRADecraft TO CREATE CONFUSION AND INSTABILITY

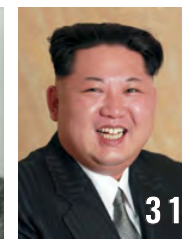


Various elements of espionage tradecraft used by underworld operators continue apace across many theatres. In Montenegro, it appears Russian Intelligence were involved in a plot to assassinate the country's leader and overthrow his government; in Cuba, an agency has opted to use sonic weapons against US diplomats, while in troubled Ukraine, a plot has been exposed resulting in Kiev being blamed for helping North Korea secure weapons and missile technology. These three events are symbolic of how tradecraft can and does impact everyone - and the repercussions can be dramatic.

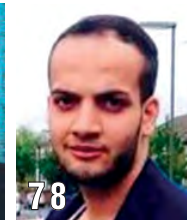
Just as troubling and impactful, the actions of ISIS and its growing band of fragmented international followers. Attacks beyond the recognised theatres of Syria and Iraq continue. Barcelona, London and other cities have all been affected. Atrocities performed in these locations come at a time when ISIS 'military' forces are being squeezed and destroyed in important locations - such as the groups de facto capital - Raqqa. Soon its land fighting capabilities will have been destroyed, but this does not mean for a moment its ideology or menace to attract new members will disappear any time soon.

And as 2018 draws nearer, intelligence eyes are still firmly locked-on to evolving events in North Korea, Ukraine, North Africa and other countries. Interesting days lie ahead.

MARK BIRDSALL, MANAGING EDITOR



HEADLINERS



•8 Milo Djukanovic •23 Alan Turing •31 Kim Jong-un •43 Maria da Graça Mira Gomes •59 Bashar al-Assad •66 Robin Stephens •71 Rual Castro •78 Yahyah Farroukh

INTELLIGENCE CHOICE

NAMING OF AN OPERATIONAL CIA OFFICER

In days gone-by, it was taken as *near* protocol that news editors would refrain from naming or identifying intelligence officers, especially if they were still active in the field or operational in one capacity or another. A simple phone call or in Britain, for example, a communication via its D-Notice office would have been almost certain to guarantee anonymity. The Internet and a global press that circulates news in seconds has changed all that. A good example can be the naming of former MI6 officer Christopher Steele - the author of the controversial 'Trump Dossier'. Eye Spy was but one of several UK media houses asked not to name him after his role and identity surfaced. However, once the story had gone 'Internet Global' (a new term used by the intelligence services), it became impossible to contain.

The *New York Times* has now angered the CIA by publishing the name of its most creative commander in the Middle East (and Afghanistan) overseeing its UAV 'kinetic kill operation' targeting ISIS and al-Qaida terrorists. The story and background in this informative report...

•20 SPY GAMES - NEW YORK TIMES AND THE CIA



INTELLIGENCE REVIEW • NEWS • DIGEST

ENGAGED: TALON

New Scotland Yard Introduce Vehicle Counter-Terrorism Measure

Following a spate of terrorist attacks using vehicles, New Scotland Yard has green-lighted the use of a new counter-measure called Talon. Security officials recognise that ISIS propaganda and information provided via several supportive websites, has influenced its followers to use this relatively cheap and effective method to create mayhem. 'Intelligence'

advice by ISIS asks that three rules be followed: 1. 'Secure a vehicle... 2. search a date for a special event... and 3. select a busy location'.

Counter-terrorism experts note such attacks do not necessarily require much preparation. In most cases they are low-cost and affordable. More worrying, analysis has shown many incidents are spontaneous. The new counter-measure is a road covering 'net' with inbuilt tungsten steel spikes intended to puncture

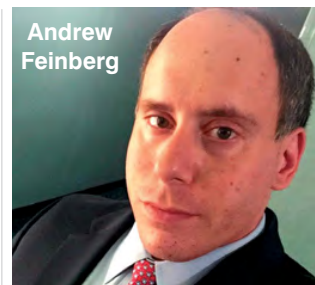
FBI EYES ON SPUTNIK

Questions Raised Concerning Russian Media Company

The FBI is reportedly investigating the Russian news agency Sputnik, after allegations the government-funded agency is acting as an "undeclared propaganda arm of the Kremlin in violation of the Foreign Agents Registration Act (FARA)."

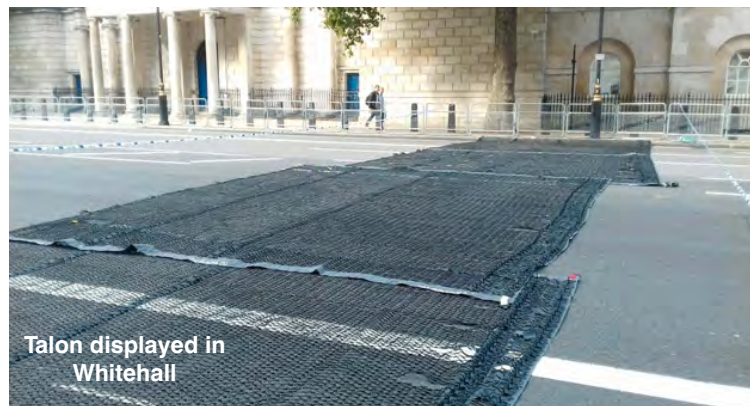
Andrew Feinberg, a former White House correspondent for Sputnik was questioned for over two hours and delivered a computer data stick containing thousands of documents he secured before being fired by Sputnik in May. Feinberg's departure follows his refusal to question the President's Press Secretary concerning a

Andrew Feinberg



COURTESY: ANDREW FEINBERG

discredited Fox News report in a televised briefing. Feinberg has since been interviewed by the FBI. "They wanted to know where my orders came from and if I ever got any direction from Moscow," he said. "They were interested in examples of how I was steered towards covering certain issues."



Talon displayed in Whitehall

tyres and disable front wheels. Officials say the system is designed to ensure the vehicle skids in a straight line and comes to a controlled stop reducing risk to crowds. Talon can be deployed extremely quickly (60 seconds) by just two officers. Sources claim it can effectively stop a vehicle weighing up to 17 tonnes. It is of course just one measure which

can protect large crowds at public events. Talon was first seen in September at the Naval Association Parade in Whitehall, London.

Chief Inspector Nick Staley of the NSY's Protective Security Operations Unit said: "This equipment undoubtedly has the potential to save lives and is just one of a number of measures



Tourists in Westminster



2008. Bulldozer attack in Jerusalem

Feinberg made his allegations on 26 May, the day he left Sputnik. He has since claimed the Russian media arm also pressured him to ask questions that suggested the Syrian regime of President Bashar al-Assad (a staunch ally of Russian President Vladimir Putin), was not behind chemical attacks in that country.



FBI Director Christopher Wray assumed his position in August

being taken to provide protection to crowds attending major events in London and reassuring businesses, workers and visitors as they go about their daily lives.”

Talon, described as a ‘super stinger’, is expected to be utilised by police forces across the country.

- Several ‘vehicle mitigation barriers’ have also been installed on nine London bridges and a number of other sites across the city following recent terrorist incidents at Westminster and London Bridges.



Leading edge consists of a barrier of spikes

COURTESY: NEW SCOTLAND YARD/CROWN COPYRIGHT

A GATEWAY TO SECRETS

The Subtle Hamas Operation to Strip Away IDF Security Layers

Earlier this year, the Israeli Security Agency (ISA), better known as Shin Bet, revealed the military wing of Hamas attempted to spy on Israeli soldiers and obtain personal information from their social media accounts. Hamas used stolen photographs of women to create fake social profiles in a bid to lure the troopers to interact. At the time an IDF source said: “These figures successfully fooled soldiers and led them to speak out about confidential issues.”

Another ruse tricked soldiers into downloading a messaging app, including a video programme that effectively turned a cell phone into a spy phone enabling data and real-time conversations with ‘third parties’ to be secured. This included personal banking details, credit card numbers, and addresses. Both male and female soldiers were targeted and to make the ruse seem more credible, Hebrew slang was used.

One IDF soldier who was tricked said: “Our connection got stronger

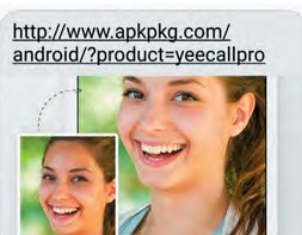


over time and trust set in. She told me she served in the army prison unit. In time, I knew it was not a woman but Hamas.”

After the intelligence organisation learned of the activity, the Israeli Army opted to conduct tests and determine the responses of its soldiers to spying attempts through social media. Some results have been released.

According to intelligence sources in Tel Aviv, 350 Israeli soldiers received ‘Friend’ requests using the method allegedly employed by Hamas - some were from “beautiful women on Facebook.” The ISA said only 6 per cent of the requests were accepted.

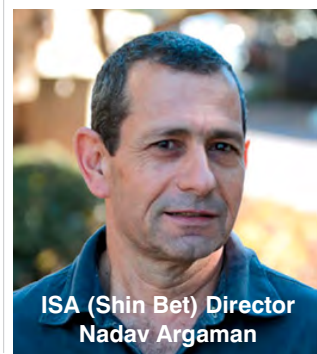
“This rate is low,” said a Shin Bet officer speaking on the condition of anonymity, “but it could be very dangerous as the enemy could reach senior people and secure sensitive information. It would just take one ignorant person among



the soldiers to cause a lot of damage to the whole Israeli security system,” he added.

In respect of other activities involving Hamas, the ISA has uncovered a complex system used by the group to transfer monies from two centres in Gaza and Turkey to its command centre in Hebron. This involves the use of couriers who pose as businessmen. A number of arrests have been made.

In 2001, a 16-year-old Israeli man was lured to the West Bank by a ‘woman’ who he met on an Internet web set. When he decided to meet, in the occupied territory, he was shot dead by a waiting gunman.



ISA (Shin Bet) Director Nadav Argaman

THE SURVEILLANCE VAN FBI INTELLIGENCE SURPRISE



Ginter Senfeldas, from Carey, North Carolina, was interested in buying a truck and stumbled upon one listed on a US Government auction website. He duly bought a 1989 Dodge Ram 350 listed with only one owner and 23,500 miles on the mileage clock; when he took delivery, Senfeldas was a little surprised with what he found inside.

The van had been used by the FBI as a surveillance vehicle and it came equipped with

radar, an intercom, surveillance tapes, notebooks, television monitors and video recording equipment, amplifiers, a toilet, handcuffs, binoculars, customised locks, plus other gadgetry. He also discovered he could turn off the engine from the rear.

Senfeldas also found microphones covertly concealed on the exterior of the vehicle. "We found out that there are hidden microphones - when we took the side markers out of the van, we found them inside the headlights and

taillights," he said. "There are little holes everywhere." Included in the paperwork were work orders from the company that originally re-fitted the van, FBI purchase papers from the dealership and owner guides for all the equipment.

Senfeldas decided to sell the van, with a Blue Book value of around \$1,500.00, listing it on eBay beginning at \$15.00. The auction ended with 47 bids and sold for \$18,700. It's not known if the Bureau participated in the auction.

CIA AND ARTIFICIAL INTELLIGENCE

Langley Developing AI Programmes to Enhance Analysis Capabilities

According to information revealed by Dawn Meyerriecks, the Deputy Director for Technology Development with the CIA, Langley currently has 137 different Artificial Intelligence (AI) projects underway to process the huge amounts of data collected from a variety of sources, including partner organisations and Open Source (OS).

The CIA, which operates various well-staffed analysis branches, recognises that AI has more access to data and a greater

ability to sort, analyse and process than analysts. And though human analysis will never be replaced, the Agency notes the increase in data collection may

become simply too voluminous for staffers to cross reference, sift and deposit. Now the CIA is focussed on creating technology capable of extracting, sorting, and



analysing data faster than any human or other computer data system. A major part of the AI system will focus on information uploaded on the Internet (Open Source). "What is new is the volume and velocity of collecting social media data," said Joseph Gartin, head of the CIA's Kent School.

THE MOSSAD 'SPY ROCK'

Surveillance & Photographic Device Discovered

Reports in the Middle East claim an Israeli 'spy rock' has been discovered by Lebanese Army troops in Kfarchouba, a few miles from the Lebanese-Israeli border and approximately 100 miles south-east of Beirut.

The device, described as "sophisticated spying equipment," had been placed in direct view of a major Lebanese military outpost which overlooks northern Israel and the eastern sector of the strategically important Golan Heights.

The Lebanese Army's intelligence corps was asked to investigate. After the rock was opened, technical experts discovered a canister with various wires and components. Ultimately, officials determined these were part of a



"sophisticated thermographic camera." Photographs posted on several Lebanese websites allegedly show the device found inside the rock - which appears to bear Hebrew writing.

It's not the first time Israeli spy devices have been discovered in Lebanon. In 2015, Lebanese troops dismantled a surveillance camera which had been carefully concealed in a concrete-type mixture and hidden amongst other rocks on a hillside near Ban Hayan. Besides an infrared camera, investigators discovered a transmitting device.



The spy camera and transmitter discovered in 2015 overlooking the Golan Heights

It's not just the CIA endeavoring to create functional and trustworthy AI platforms, Russian President Vladimir Putin recently said: "Whoever becomes the leader in this sphere [AI] will become the ruler of the world."

DAWN MEYERRIECKS

Dawn Meyerriecks left her post at the Office of the Director of National Intelligence in 2013 for a technology-related position with the CIA's Directorate of Science and Technology.

From 2004 to 2006 she had worked as AOL's Senior VP for product technology, where she was responsible for developing consumer-facing products, including the relaunch of AOL Instant Messenger, aol.com and



Messenger's open-client platform.

Meyerriecks spent a decade at Defense Information Systems Agency as chief technology officer of its Joint Interoperability and Engineering Organisation and worked at NASA's Jet Propulsion Laboratory as a senior engineer prior to her time at DISA.



Alleged Mossad camera recently discovered by Lebanese troops hidden in a rock

AIRPORT SURVEILLANCE



Paris Orly Airport

A French border police officer identified only as 'Charles D.', has been charged with espionage for supplying Moroccan intelligence agents with classified information concerning France's border-control policies and procedures; plus the movements in France of Moroccan nationals and senior Algerian government officials. Court documents state Charles D. provided classified documents from the Direction centrale de la police aux frontières (DCPAF), to a man identified only as 'Driss A.', who worked at Paris Orly Airport in a security capacity.

At Driss A.'s residence, photographs of various Algerian officials were recovered. Sources believe they were supplied by an intelligence officer at Algeria's Embassy in Paris enabling the operative to identify the men for surveillance purposes.

It transpired that Driss A, a Moroccan-born French citizen, was secretly employed by the Deuxième Bureau, Morocco's military intelligence service. In return for his secret work, the agency compensated Charles D with free holidays in Morocco.



COURTESY DIRECTION CENTRALE DE LA POLICE AUX FRONTIÈRES (DCPAF)



THE PARK BENCH PLOTTERS

Trial begins of pro-Russian plotters in alleged attempt to assassinate Montenegro Prime Minister Milo Djukanovic

Fourteen people have been accused of an Election Day plot (16 October 2016) to overthrow the government and assassinate the Prime Minister including two Russians, nine Serbians and three Montenegrins. Four of the men are being tried in absentia: among them, two Russian intelligence officers accused of masterminding the plot.

Authorities in the Montenegrin capital Podgorica, collected evidence during an undercover operation that they say show “nationalist structures from Russia” were behind the plan to oust Prime Minister Milo Djukanovic. “Now we know that Russian state bodies were also involved,” said Chief Special Prosecutor Milivoje Katnic speaking to journalists on state television.

**City Hall (parliament building)
- location of the proposed
coup and assassination**



Prime Minister Milo Djukanovic

The story surfaced in November 2016, though went largely unreported due to a lack of information flow. However, senior Whitehall and NATO sources said the plot appeared to be genuine and was orchestrated by Russian intelligence officers with backing from Moscow. At the time, the main charges against the plotters, described as a “Serbian paramilitary force,” centred upon terrorism offences. There were tentative suggestions of a Russian link, but at the time Katnic said:



2016. Former US Secretary of State and Montenegro Prime Minister Milo Djukanovic at NATO headquarters. Some intelligence watchers believe the plot was enabled as a last ditch attempt to stop the country joining the security organisation

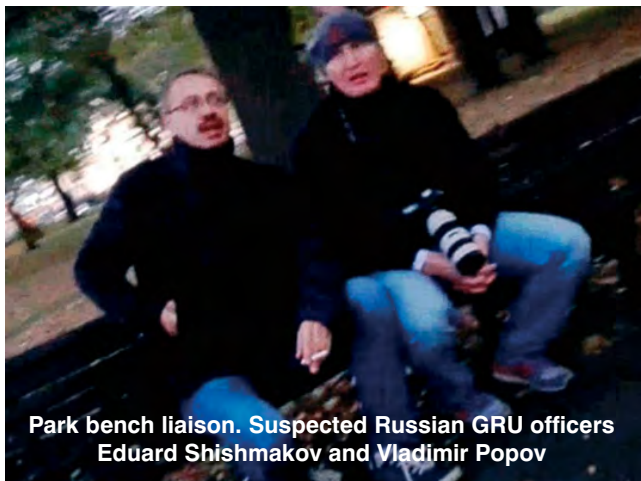
“We don’t have any evidence that the state of Russia is involved in any sense, but we have evidence that two Russian nationalists were the organisers.” Now photographs, released by Montenegro officials, have surfaced via an unnamed European security service that appear to support claims that Moscow played a central, but covert role in the plot.



The imagery, taken at the time of the coup, show two Russians accused of plotting the operation. The men have been named as Eduard Shishmakov, 46, and Vladimir Popov. Both are said to be members of Russia’s GRU (military intelligence). In one photograph, Shishmakov is pictured meeting with a Serbian national called Aleksandar Sindjelic. He was subsequently arrested and has reportedly confessed his involvement in the attempted coup and admitted working as an agent for the two Russians. ➤



Embassy of Montenegro, Warsaw, Poland. Intelligence was forwarded here on one of the two GRU officers involved in the plot



Park bench liaison. Suspected Russian GRU officers Eduard Shishmakov and Vladimir Popov



1. Shishmakov pictured with 2. Aleksandar Sindjelic



Russian Embassy, Warsaw

Sindjelic has reportedly admitted receiving a large amount of money to purchase weaponry and other “provisions” including police uniforms that were to be worn by coup associates. He also said that on one occasion whilst visiting Moscow in preparation of the operation, he was subjected to a polygraph test by the GRU.

Another photo shows Shishmakov and Popov together on a park bench believed to be in central Belgrade in neighbouring Serbia.

THE OPERATION

The plan was to infiltrate a pro-Russian rally outside the Parliament building in the capital Podgorica. The



Vladimir Popov

plotters, dressed as policemen, would break into Parliament and turn their fire on the protesters, thus making it look like Montenegrin state security had shot its own people. Part two, and in a separate action, the pro-European Prime Minister



SHIROKOV, EDUARD
WANTED BY THE JUDICIAL AUTHORITIES OF MONTENEGRO FOR PROSECUTION / TO SERVE A SENTENCE
IDENTITY PARTICULARS

Present family name: **SHIROKOV**
Forename: **EDUARD**
Sex: **Male**
Date of birth: **20/02/1971 (46 years old)**
Place of birth: **G.Cita, Russia**
Language spoken: **Russian**
Nationality:



An Interpol notice identifying Eduard Shirokov. Right: Shishmakov pictured in a Russian Navy uniform at a diplomatic event in Poland 2014

Djukanovic would be assassinated in the hope of a pro-Russian politician seizing power.

Montenegro officials supported by Western intelligence chiefs believe one of the aims of the coup attempt was to prevent the country joining NATO. * Milivoje Katnic, said: “We now have the evidence that nationalistic structures from Russia are behind the coup attempt, but also that certain state bodies of Russia are involved on a certain level.” One piece of evidence that will be presented in court concerns certain software in a number of cell phones used by the plotters. This is said to



Chief Special Prosecutor, Milivoje Katnic

have allowed the operatives to call and receive messages safe in the knowledge that the communications could not be intercepted. Eye Spy also understands the security services in the country discovered payments (around \$200,000) made by the Russians to certain individuals in the spy ring.

Asked about his country’s supposed involvement in the coup and assassination plots, Russian Foreign Minister Sergei Lavrov said: “For anyone to connect Russia to these events is absurd. We have not been presented with a single fact.”



Suspects arrive in court as the trial begins



Russia's Foreign Minister Sergei Lavrov called the allegations "absurd"

For the best part of a decade Russia has opposed Montenegro's plan to join NATO. A popular destination for Russian tourists, the country, which has a tiny population of around 650,000 is effectively split between those seeking closer ties to the West, and others (the majority) wanting to maintain links with Moscow.

The trial will be the largest in Montenegrin history and believed to be the first time serving GRU officers have been charged with terrorism offences and criminal activity in a European country.

COVER AND LEGEND

Interestingly, though both Shishmakov and Popov are back in Moscow, Polish Intelligence confirmed Shishmakov, a captain in the Russian Navy, had been deported from the country in 2014 for espionage activities after declaring him 'persona non grata'. He worked as a deputy military attache at the Russian Embassy in Warsaw using a passport in the name of Eduard Shirokov. Eye Spy believes both MI6 and the CIA assisted Montenegro with its investigation.

*Montenegro split from Serbia in 2006. It became the 29th member state of NATO in June this year.



Edward Shirokov is a supposed pseudonym of one of the two Russian GRU spy handlers

ECHOES OF THE COLD WAR

Russia Ordered to Shut Down its San Francisco Consulate



In an action reminiscent of happenings during the Cold War, the United States has instructed Russia to close its consulate in San Francisco. The tit-for-tat move comes just weeks after Moscow demanded that Washington reduce the number of diplomatic staffers at its sites in Moscow by 755. US Secretary of State Rex Tillerson contacted his Russian counterpart Sergei Lavrov by telephone notifying him of the decision.

Though seen as yet a further disintegration of relations between the countries, Tillerson said the decision was taken to create "parity between the countries" - around 450 people now work in each respective overseas post. And whilst Lavrov expressed "regret at the escalation of tension in bilateral relations," the move was expected. The editor of a state-



Anatoly Antonov



owned newspaper from Russia's pro-government media admitted the Kremlin would not respond with "hysterical outbursts." The closing of the consulate coincided with the arrival of Russia's new ambassador to the United States, Anatoly Antonov. He said, "it's necessary to sort things out calmly."

America's mission was reduced primarily as a response to the continued investigation and sanctions imposed following Russian interference in the 2017 US General Election. Former US ambassador to Russia, Michael McFaul, admitted the removal of the US staff compared to America's action will have more impact on the United States.

The San Francisco operation was very important to Russia. Intelligence officials note its proximity to Silicon Valley and other business sites. The FBI had a dedicated unit monitoring supposed diplomatic staff at the consulate, many of whom are suspected of corporate espionage and cyber activities. Former CIA official Steven Hall, said: "I would assume they were using that as a base for intelligence operations in the Bay Area and Silicon Valley."

Police guard a road leading to Barcelona's famous Las Ramblas boulevard moments after a terrorist had driven into holidaymakers and civilians, killing 15 people in total



BARCELONA TERRORIST

Controlled ISIS terrorist cell resort to simple attack method after plot to strike a multitude of targets undone by accidental explosion. MI6 just one of a number of intelligence services engaged in worldwide search for similar cells intent on mass casualties

On 15 August, a major explosion occurred at a house in the town of Alcanar, approximately 120 miles south of Barcelona. Initially believed to be a simple accident, the blast - which totally destroyed the residence - was the result of dozens of gas cannisters and bottles containing propane and butane exploding.

Police and firefighters attended the scene and two bodies were recovered from the rubble - identified as Abdelbaki Es Satty, 45, and Youssef Aallaa; at least five persons in the building were injured.

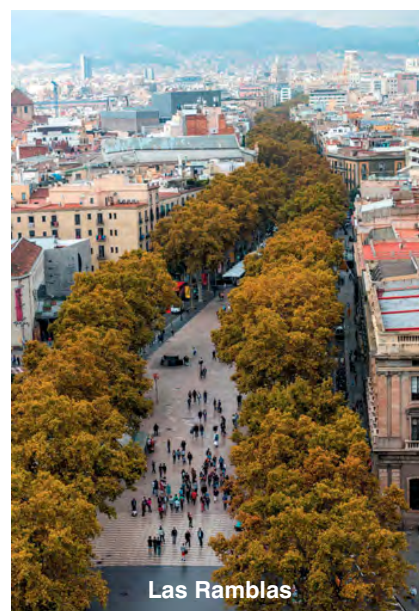
It was not until the following day did investigators consider the event suspicious - this after a terrorist killed 15 people in Barcelona using a hire van to attack civilians. It transpired Aallaa was an explosives' expert and Es Satty

the purported head of a twelve-man ISIS terrorist cell. A third person, Mohamed Houli Chemlal, who had been taken to hospital, was immediately detained. It is now believed he was the cell's primary bomb-builder.

Spanish Intelligence believes the accidental detonation of an estimated 120 gas cannisters forced the rest of the terrorist gang to alter the modus operandi of their attack and turn to a more rudimentary method to inflict casualties.

THE ATTACK - 16 AUGUST

As in previous incidents involving the use of vehicles to attack civilians* the ISIS cell selected one of the most popular and busy locations in Barcelona - Las Ramblas. The primary attack vehicle, a white Fiat van, was driven by Moroccan-born Younes Abouyaaquob, 22. At 4.50pm he began his



Las Ramblas

attack outside the Placa de Catalunya Metro Station before moving to Las Ramblas. Here he crashed into dozens of people as he zig-zagged across the busy boulevard in a near minute-long - 500 yard action - which resulted in 13 deaths and left more than 100 needing hospital treatment for their injuries. The van



Armed police and emergency services assemble at the Metro station - Las Ramblas

T ATTACK

was soon surrounded by angry people, but despite people pursuing the attacker, he exited the area on foot via La Boqueret market and managed to avoid police. CCTV images

showed the killer calmly walking away from the scene, seemingly unconcerned about his previous actions. Another hire van linked to the gang was found in the town of Vic, 50 miles north of Barcelona. Police believe it had been strategically positioned and was intended to be used as an escape vehicle. This had been hired on the same day as the vehicle used in the Barcelona attack. ➤



Cell leader, attack driver, bombmaker and van hirer

L-R clockwise: Abdelbaki Es Satty, Younes Abouyaaquob, Mohamed Houli Chelmal and Moussa Oukabir



An armed police officer near Las Ramblas moments after the attack



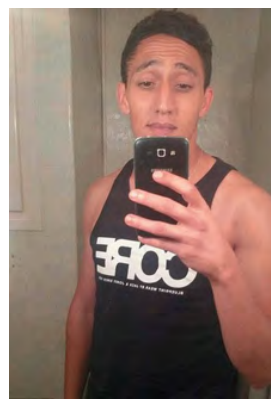


A police officer and the Fiat Talento Kombi van used in Las Ramblas attack - a victim lies in front of the vehicle - 15 people succumbed to impact injuries

Spanish security officials authorised the immediate erection of vehicle stop barriers and patrols on roads in and out of the city, other police forces in neighbouring towns were also placed on alert. A vehicle crashed through one such checkpoint at Sant Just Desvern on the outskirts of Barcelona and struck a police officer breaking her leg. The car was later abandoned a few miles away; inside the body of a man later identified as Pau Perez, a civilian, was found. He had been stabbed to death by Abouyaaquob who had reportedly stolen his car; the lead terrorist was still at large. By now, images of Spain's most wanted were being circulated across the world. As a footnote to this incident, some journalists stated Perez had been shot dead by police - reports denied by Spain's Interior Ministry but this part of the investigation continues today.

CAMBRILS INCIDENT

Approximately eight hours later (1.00am) and a little over 60 miles south of Barcelona, a



Driss Oukabir surrendered to police after his identification papers were discovered in the Las Ramblas attack vehicle and his photo widely circulated

(believed to be a female and not named for personal security reasons) confronted the gang who refused to accept her command to

black Audi vehicle struck more pedestrians in the town of Cambrils. A 63-year-old woman was stabbed to death. The car eventually overturned and stopped. Five young men exited - and at least three wore what appeared to be suicide explosives' belts. A single Spanish police officer

THE ISIS CELL RECRUITER Abdelbaki Es Satty

Terror cell leader Abdelbaki Es Satty had been jailed for drug smuggling in 2010 and was told he would be deported in 2014 when he was released. However, he fought the ruling, claiming the order would be a breach of his human rights - and the court agreed. Thereafter he sought asylum - and won - a decision which allowed him free passage and movement to all 26 European countries which operated in the Schengen area.



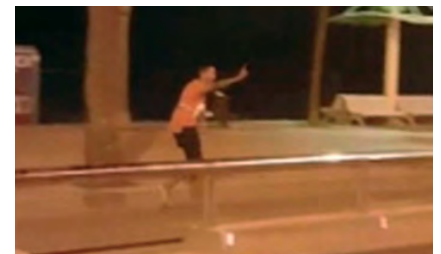
It was during his time in jail, he became friends with an al-Qaida bomber.



Las Ramblas attacker Abouyaaquob is caught on CCTV as he calmly departs the area



Police assist an injured civilian following the attack



A terrorist wearing an unfinished suicide bomb belt flees his vehicle in Cambrils - moments later he was shot dead



Passeig maritim, Cambrils. Exact location of the second TAV. Inset: The vehicle used in the Cambrils attack is taken away



Las Ramblas is a famous boulevard and entertainment area which runs through the centre of Barcelona for approximately one mile. Hugely popular with tourists and locals alike, the street begins at the Placa de Catalunya (Catalonia Square) to the seafront and Christopher Columbus monument

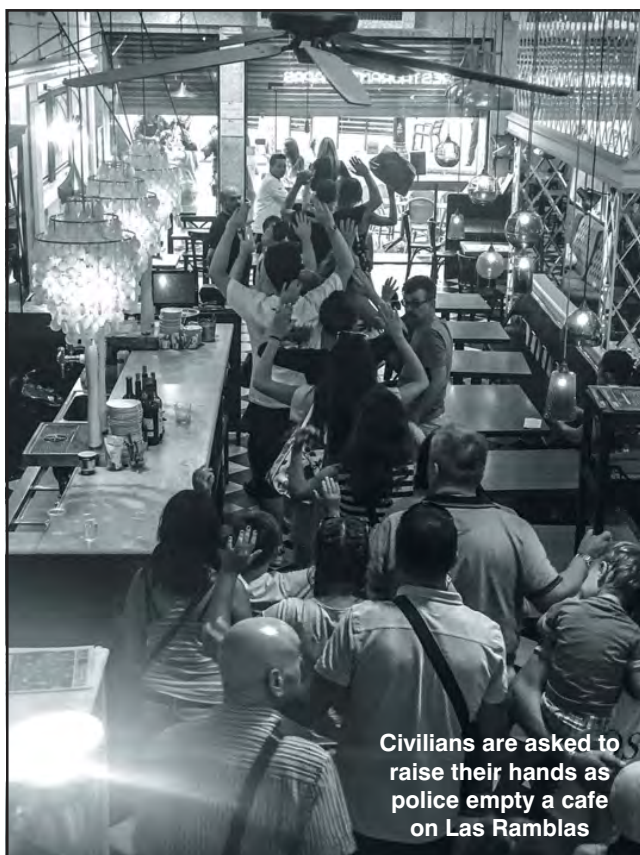
surrender. Four were shot dead, but the fifth man escaped. However, like his comrades, he too would soon be shot dead. Police later named the deceased as: Said Aallaa, 18; Mohamed Hychami, 24; Moussa Oukabir, 17; Omar Hychami and Houssaine Abouyaaqoub. A note written by one of the attackers and recovered in the Cambrils safe house, offered

'apologies' for what they were about to do. Oukabir's elder brother, Driss, 28, was also arrested. He denied being part of the cell, but curiously admitted hiring the two vans used in the operation. Driss Oukabir told police: "I though they were for moving homes." His passport was discovered in one of the vans. (Some sources claim his younger brother

Moussa stole his driver's licence and other identification papers enabling him to hire the vans).

END GAME

On 21 August and a little west of Barcelona and north of the terrorist cell's Alcanar safe



Civilians are asked to raise their hands as police empty a cafe on Las Ramblas



Counter-terrorism specialists secure Las Ramblas boulevard



Sagrada Familia basilica - Barcelona - ISIS target

house, police received a number of calls from residents living in Subirats. They reported a man matching Abouyaaquob's description had been trying to gain access to several houses. Within minutes armed police arrived - but again - Abouyaaquob avoided detection, this time by fleeing into a major vineyard. However, the terrorist, who had now donned what appeared to be an explosives' belt, was trapped. When confronted by two officers he shouted "Allahu Akbar." Moments later he was shot dead. Police recovered a bag full of knives at the scene.

Intelligence officials in Spain are convinced the sheer number of gas cannisters destroyed at the Alcanar safe house suggest the terror cell was planning to strike a much larger target. Indeed, evidence secured from the building, data from electronic media and statements made by some of those detained, indicate the primary target may have been Barcelona's famous Sagrada Familia basilica (church). Mohamed Houli Chemlal also confirmed Abdelbaki Es Satty an imam, was the head of



Three cell members pictured at a petrol station just hours prior to the attack in Cambrils

the cell who along with most of the terrorists lived in Ripoll, north of Barcelona. Es Satty is known to have links to some al-Qaida operatives and may well have played a pivotal role in influencing others to join his terror cell.



ATTACK CASUALTIES



Primary areas of Catalonia attack sites and operations

Sixteen civilians died in the attack, most were tourists, including the youngest victim, 7-year-old British-Australian national Julian Cadman. Another casualty was father-of-three Jared Tucker, 43, an American on honeymoon with his wife. In total, nationals from 24 countries were either killed or injured.



Julian Cadman

nationals from 24 countries were either killed or injured.



© JIMMY BAIKOVICIUS

TAV

A GROWING TREND

Eye Spy met with a NYPD counter-terrorism official in early 2016. He explained that ISIS/Daesh had initiated a new programme concerning the use of vehicles to attack civilians and security services. Through encrypted channels its senior men had contacted operatives and supporters in Europe providing them with details and guidance on how to perform such acts. "These instructions had been intercepted by the NSA and circulated to associate intelligence organisations," he said.

14 JULY 2016. NICE, FRANCE. A truck driven by Tunisian Mohamed Lahouaiej-Bouhlel rammed into crowds on the Promenade des Anglais killing 86 people.

19 DECEMBER 2016. BERLIN, GERMANY. Tunisian Anis Amri crashes a stolen truck into festival goers at the Christmas Market at Breitscheidplatz. Twelve people are killed.



8 JANUARY 2017. JERUSALEM, ISRAEL. Fadi al-Qanbar, an Arab-Israeli drove a truck at a group of Israeli military cadets killing four and wounding several others.



TERRORIST ATTACK BY VEHICLE



The aftermath of a TAV in the centre of Stockholm, Sweden

By October of last year, dozens of 'informative' features written by ISIS weapons and explosives instructors started to appear on the Internet. Primarily the attack method, known as TAV in the intelligence world, was developed because some ISIS supporters

had complained securing weaponry and bomb-making materials was simply too difficult.

One of the first attacks, however, was in Nantes, December 2014. Here a van crashed into civilians enjoying the Christmas market.

Though no fatalities occurred, 20 people were seriously injured.

Outside of the Iraq, Syrian and Libyan theatres, a number of major attacks using vehicles, from saloons to 40-tonne trucks have taken place in Europe.

22 MARCH 2017. LONDON, UK. Briton Khalid Masood drives his vehicle into pedestrians walking on Westminster Bridge. He then stabbed unarmed police officer Keith Palmer to death.



7 APRIL 2017. STOCKHOLM, SWEDEN. Five people are killed after Uzbek Rakhmat Akilov attacked using a large truck.

3 JUNE 2017. LONDON, UK. Eight people died when three attackers, Khuram Butt, Rachid Redouane and Youssef Zaghba struck pedestrians on London Bridge before stabbing several civilians in nearby Borough Market.

19 JUNE 2017. LONDON, UK. A lone wolf terrorist in the person of Darren Osborne drove a van into worshippers outside a mosque in Finsbury Park. One person died in the attack.

9 AUGUST 2017. PARIS, FRANCE. Algerian Hamou Benlatrenche struck a group of soldiers with his car injuring six. He is duly arrested.



Anti-vehicle attack blocks on London Bridge. Inset: Dresden, Germany



The King of Spain, Felipe VI, President of Catalonia Carles Puigdemont and Mayor of Barcelona Ada Colau attend a wreath-laying ceremony at Las Ramblas

One police source said the imam was “responsible for radicalising most, if not all of the men.” Sources also claim he once shared a prison cell with one of the AQ terrorists responsible for the 2004 Madrid train bombings which left 191 people dead. And it was during this time he became radicalised.

ISIS soon celebrated the attacks. In an Internet message posted by the group’s Amaq ‘news agency’, it called the attackers ‘soldiers of the Islamic State’. Another post promised more attacks in Spain and told its supporters the country will be returned to the ‘land of the Caliphate’. British intelligence sources are dubious of such claims - noting many acts are performed by supporters of ISIS ideology - not operatives controlled by commanders or authorised to act. However, Eye Spy believes this attack may well have been the result of inter-action linked to other gang members and

a wider European network of jihadis. Indeed, just prior to the attacks, Abouyaaquob is known to have driven from Barcelona to Paris. The purpose of that journey remains unknown.

In the past three years, MI6 has engaged with various intelligence services to try and identify ‘information couriers’ and a network of ‘ISIS ghost commanders’ willing to recruit others to perform attacks outside the Middle East and North African theatres. This theatre stretches from Norway to southern European countries. Abdelbaki Es Satty, the cell leader, may well have been contacted by such an ‘actor’ despatched by ISIS from Syria or Iraq.

MISSED CLUES

Some critics of the Intelligence and security system in Spain believe important and significant clues were missed by various



A victim receives help from passers-by

authorities. For example, the disclosure of a letter written in early 2016 to Catalan Police by local security officials in Vilvoorde, Belgium. Hans Bonte the Mayor of Vilvoorde said officials had made contact with Catalan Police expressing concerns about Abdelbaki Es Satty, who had been appointed imam in Ripoll in 2015. However, officials in Barcelona state the contact was “informal” and not passed on to Spain’s or Catalan’s Interior Ministry. Despite this claim, it seems unlikely the information did not reach Spain’s National Intelligence Centre (CNI - successors of CESID) or the country’s National Cryptologic Centre (CCN).

Ironically also, that three days after the safe house blew up in Alcanar, investigators discovered various items that analysts would have immediately recognised as suspicious. A viable suicide bomb belt was discovered in the



City dignitaries and senior police officials pay tribute to the unnamed officer who bravely confronted and shot dead four terrorists in Cambrils



Mohamed Houli Chemlal and Driss Oukabir - both are charged with the Barcelona outrage

rubble along with traces of the notoriously unstable TATP explosive. The cell had purchased 500 litres of acetone used in the manufacture of the explosive. Linked to these items several bags of nails and screws along with around 20 pillow cases which were to be used in the construction of bombs. Of note, TATP has been used by ISIS in other attacks, notably Brussels and Paris.

Eye Spy understands, Mohamed Houli Chemlal, the suspected bombmaker who survived the accidental blast at the safe house in Alcanar, has imparted further information on the original attack plan. This involved the hiring of multiple vans and attack locations.

Spain's Prime Minister Mariano Rajoy condemned the attack and announced three days of mourning. World leaders joined their Spanish counterpart and offered support.

* Eye Spy has been informed the new terminology or acronym for such events is TAV (Terrorist Attack [by or using] Vehicle).



Messages of condolences from visitors around the world

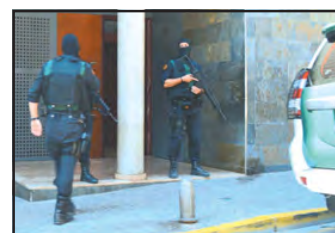


The terror cell secured 500 litres of Acetone used in the production of TATP - a highly volatile explosive which can easily explode if subjected to violent movement, heat and even friction. Inset top: The destroyed safe house. Inset lower: Acetone peroxide crystals



INTEL INSIDE

Spanish security forces have detained several people operating on behalf of ISIS in the last two years. Weapons and explosives have also been seized, but despite this, intelligence watchers believe the country is being used as a distribution channel to arm terror cells across Europe. Similar passages exist in Turkey and other southern European states. This photo shows armed police following the detention of two men in Arbucies suspected of channelling funds to the group



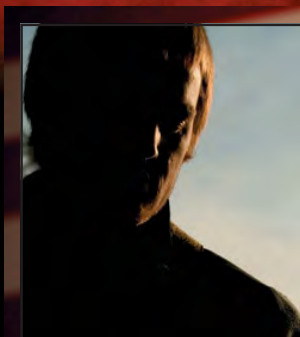
OVERFLIGHTS • TARGETS • KILL MISSIONS • CONTROVERSY

SPY GAMES

New York Times Criticised for Naming Covert Officer TAKING COVER FROM THE CIA

America's *New York Times* has defended its decision to reveal the identity of one of the CIA's most experienced officers embedded in the Middle East. Its explanation has not satisfied the CIA nor a watching public, as evidenced by a backlash on social media.

CIA Director Mike Pompeo criticised the newspaper after it named the officer calling him 'chief of operations' in a June feature and said he was tasked with 'weakening al-Qaida'. The officer was still working undercover which made publication an "unconscionable decision," and "jeopardised his future role as a covert officer" Pompeo said. Insider's said the officer, whose name Eye Spy has chosen not to publish* was a leading contender to head the Agency's Iran Desk.



CIA Director Mike Pompeo - deeply concerned that an operational area commander has again been referenced in connection with a covert UAV programme

BACKGROUND

As the newspaper prepared a summer feature on intelligence happenings in Iran (including naming the officer), its editorial contacted Langley for comment. The CIA asked that it not publish his name, citing a number of reasons, including the fact that he was working undercover. Despite the discussion,

the NYT chose to publish his name anyway in a 2 June feature.

Now its editorial has explained the decision - in a statement issued by the newspaper's national security editor Amy Fiscus: 'In this case, editors decided to publish the name because [the agent] is a senior official who runs operations from the Agency's headquar-



Left: Abu al-Khayr al-Masri, 59, killed by a CIA-controlled UAV in Syria in February 2017. The al-Qaida commander and son-in-law of Osama bin-Laden was connected to the 1998 African US Embassy bombings. He is but one of a number of known terrorists believed to have been killed in the covert CIA Kinetic Kill Programme



The Northrop Grumman RQ-4 Global Hawk is widely used by the US military and the CIA. Remarkably, this powerful surveillance and intelligence platform will celebrate its 20th year of flight next year



-ters outside Washington, not in the field. He is also the architect of the CIA's programme to use drones [UAVs] to kill high-ranking militants, one of the government's most significant paramilitary programmes. We believe that the American public has a right to know who is making life-or-death decisions in its name.

'It was not the first time that [the agent's] name has been mentioned in our newspaper. After his identity was disclosed in a 2015 article, The Times' executive editor, Dean Baquet, discussed the rationale in an



Former CIA Deputy Director Mike Morell



WikiLeaks advertising truck outside The New York Times headquarters

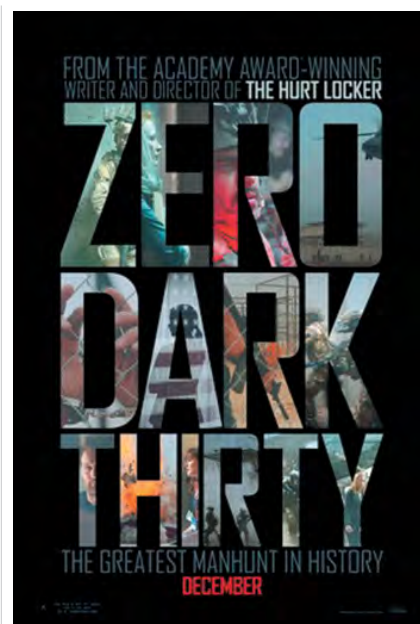
interview with Lawfare, a website that covers national security law, and gave more insight into editors' decision-making'.

The explanation appeared in the newspaper's Resource Center, an organ described by its owners as 'a newsroom initiative that is helping The Times build deeper ties with our audience'.

COUNTERTERRORISM SPECIALIST

For the record, the officer was first named in a *New York Times* story concerning his central role in America's covert UAV programme operating in the Middle East. He joined the Agency around 1980 and rose to head the special Counterterrorism Center (CTC). He has been dubbed the 'Dark Prince' and 'Ayatollah Mike' due to his work in the Middle East.

Eye Spy was informed the officer, aged 58 and said to use the cover name 'Roger', is still connected to current operations in and around Iran.



The CIA officer is reportedly the inspiration for 'The Wolf' in the motion picture - 'Zero Dark Thirty'

CODEBREAKER'S REVEALING COMMENT?



WWII. Turing (far left) with colleagues enroute to Bletchley Park

ALAN TURING'S LOST LETTERS

Letters, notes and correspondence discovered inside a filing cabinet at the University of Manchester, offer a unique insight into the life of Britain's most famous WWII codebreaker Alan Turing. Dated between 1949 and 1954, a few papers also relate to Turing's research and views, some of which the UK's closest ally, the United States, may view with dismay.

Some 148 documents were found inside a cabinet at Manchester's School of Computer Science in a paper folder marked simply 'Alan Turing'. The folder would have been filed when Turing was Deputy Director of the Computing Laboratory. The documents are all handwritten and include a letter to GCHQ requesting a photo for the history of Bletchley Park, as well as a copy of a draft radio programme dated 1951 on artificial intelligence entitled 'Can machines think?'.

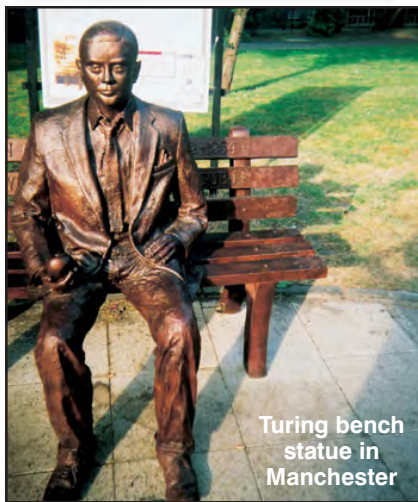
Archivist James Peters said: "There is very little in the way of personal correspondence,



Turing's mug still hangs chained at Bletchley Park Museum

and no letters from family members, but this still gives us an extremely interesting account and insight into his working practices and academic life whilst at the University of Manchester. There is really nothing else like it."

The file also contains a number of invitations from American universities such as MIT, for visits and lectures. An example of an exchange dated 20 Feb 1953: From physicist Donald Mackay, King's College London. He asks about the 'Macy meeting this spring', [he is referring to the Macy cybernetics conferences in the US, the 10th and final one being held in April 1953]. Turing's says he has



Turing bench statue in Manchester



already written to Warren McCulloch, who organises the conferences, to say he won't be attending. And even though he admits the meeting has appeal: 'I would prefer not to go to the United States... I would not like the journey, and I detest America'.

An unexpected comment considering the remarkable support and machinery he received from the Americans at his former base of operations - the WWII Bletchley Park codebreaking centre.



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



CRYPTOCURRENCIES A PRIMARY TOOL OF ESPIONAGE

Cyber Specialist and Eye Spy
Associate Editor Kevin Coleman
examines Cryptocurrencies and
their growing relevance to the
funding of espionage and intelli-
gence operations... as well as
underworld activities



The art of spying has certainly evolved over the years. It can be traced back to the Roman Empire that ran from 753 BC to 27 BC and again from 64 AD to 1453 AD. The tools and techniques of spying and espionage went through their own rapid revolution as well. The greatest period of change in the field of espionage was ushered in during the Internet era of the mid-to-late 90s. I certainly had a front row seat for this period with my role as Chief Strategist at Netscape, the company credited with the introduction of the web browser as well as the commercialisation of the Internet.

Now we stand poised at the inception of another technology that has already begun to have a profound impact on spying and espionage. Cryptocurrencies are the new 'piece' of technology at the centre of this evolution. Many readers may not be familiar





Moving money via the touch of a button and 'out of sight'

with the term cryptocurrency... but don't worry, you are not alone! Basically cryptocurrency is a form of value transfer that is also referred to as virtual currency, digital currency, eCash or digital money. To put the current state of cryptocurrencies in proper and easily understandable context, consider at the time of writing this the sum value of ALL (920+) cryptocurrencies is nearly \$96 billion USD [figure as of July 7, 2017]. That is more than the recent estimates for the latest annual GDP of 146 individual countries based on information contained in the CIA World Fact Book. One has to wonder what those numbers would be when you included the cryptocurrencies specifically designed and the

ones being used on the Dark Web or black market. It's likely they would be much greater.

To put such figures in perspective, at the time of writing a single Bitcoin was worth \$2538.72 and an ounce of gold \$1,227.50. Remarkable; a single Bitcoin worth more than an ounce of gold!

INTEL INSIDE

A recent cryptocurrency training programme (webinar) drew over 3,000 professionals (students) from countries around the world. This clearly shows the global interest in the topic. Cryptocurrencies are commonly in use on the Dark Web also known as Deep Web [non-indexed web sites]. The Dark Web is a part of the Internet that can only be accessible by using special applications (software) that allows users and websites to operate and conduct transactions, transfer digital files and sell special products and data in total



anonymity; such activities are untraceable and beyond the watchful eyes of the intelligence world.

Some specialists estimate the total \$ value of activities/transactions on the Dark Web (financial aspects sometimes referred to as the Shadow Economy) is currently a staggering \$10 trillion dollars. That is greater than all but three economies - China, United States of America and European Union states.

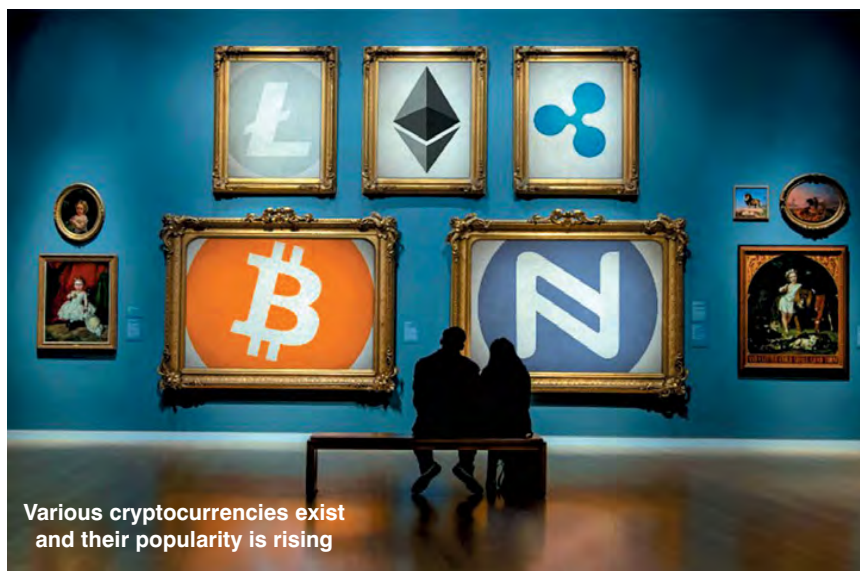
INTEL INSIDE

One study determined that the Dark Web consists of approximately 300,000 websites. Another early study suggests that the Dark Web is 400 to 550 times larger than what is indexed (the surface web). No one knows for sure the real size of the deep Dark Web.

CYBER ESPIONAGE

The quick-spreading cyber attack technique referred to as 'Ransomware' struck targets in





Various cryptocurrencies exist and their popularity is rising



A preliminary impact assessment determined the attack was causing mass disruption.

INTEL INSIDE

Early on in the ransomware attack only 26% anti-virus product/services (evaluated successfully) detected the Petya malware.

Ransomware payment is not the only use of cryptocurrencies in such clandestine operations. Funding operations, purchasing equipment, including weapons (the illegal arms trafficking market is valued at between \$6 to \$10 billion), payment to spies, operatives and sources and many more areas can benefit from the anonymous nature of cryptocurrencies and the near impossible trace of such transactions. In fact, one cryptocurrency specific to the Dark Web goes as far as to completely delete ALL records of the transaction once it is complete. ➤



Intelligence sources believe the funding of some covert operations is conducted using cryptocurrencies

Britain, France, Russia Spain, Ukraine, United States and many other countries. The WannaCry attack was the largest 'outbreak' of ransomware to date (See Eye Spy 109). The estimated total economic impact of WannaCry Ransom (\$300 USD per infected computer), plus disruption and 'clean-up' costs was between \$4 and \$8 billion. Shortly after the cyber attack a second took place dubbed Petya - leveraging ransomware (27 June 2017) sprawled across Britain, Denmark, France, Russia, the Ukraine and some firms within the United States. As always, with an attack like this a significant amount of confusion and misinformation appeared in the media. And just like before, payment demands were to be met through the use of a cryptocurrency. The ransom (about \$300) was to be paid in Bitcoin to an account identified as 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx.

The illicit moving of weapons and the illegal arms trade are worth billions of pounds each year- much of the activity is conducted via transactions on the Dark Web using cryptocurrencies





Unconfirmed reports suggest that they even over-write the area(s) where the information was digitally stored to ensure it can never be retrieved. One has to consider the degree of espionage, clandestine activities, human trafficking, illegal drugs sales, arms sales, militia financing and terrorist activity support being funded through the use of cryptocurrencies.

INTEL INSIDE

Former FBI Director James Comey, testified before US Congress, stating an increasing number of criminals are "going dark" - that is to say, obscuring their paths using technology (cryptocurrencies being one). He specifically called out drug traffickers use of virtual currencies to obscure their transactions.

ESPIONAGE AND FUNDING

Prior to the emergence of cryptocurrencies, the anonymous and untraceable transfer of money to fund spying operations, payments to spies, contacts and sources, was considered by many as the Achilles' heel by those charged with overseeing such activities. While

the pool of monies set aside for espionage purposes was kept hidden, these funds needed to somehow make it covertly from the 'funder' [controller] to those in the field. The transfer of hard currencies, both paper and electronic, had previously provided those engaged in counter-intelligence with an opportunity (to a degree) to trace the movement of money. We should also keep in mind 'marked bills' for tracing paper currency. Currently, many in the intelligence and security world are beginning to ask if paper currencies are rapidly becoming obsolete. All of this has led many organisations to spend a considerable amount of time and expense determining how best to fund operatives and operations while limiting the traceability of the funds being transferred. In the main, spies and covert operatives do not work for free. With an estimated average wage of \$40,000 to \$90,000, plus expenses incurred, operatives need to get paid clandestinely.

We must also think about all the information (and other materials) bought and sold whilst persons are engaged in the art and science of espionage. This too is a prime area for the use of cryptocurrencies. Now that cryptocurrencies have entered the intelligence equation, traceability has been greatly minimised. It is important to keep in mind



Former FBI Director James Comey

there are a number of exchanges, that for a fee, you can transfer your cryptocurrencies and have them converted to traditional forms of money - good old hard cash! You can even specify the denomination you would like. Once again it is the untraceability and security that are the primary attractive features associated with cryptocurrencies. However, not all cryptocurrencies are created equal in this respect.

INTEL INSIDE

Many consider the following five cryptocurrencies as having the highest degree of non-traceability. #1 MONERO - total value \$617,612,692; #2 ZCASH - total value \$454,997,976; #3 DASH - total value \$1,296,705,561; #4 SHADOWCASH - total value \$445,869; #5 BYTECOIN - total value \$ UNKNOWN!

NOTES: The values are based on information sourced on 1 July 2017. In May 2017, the Monero Cryptocurrency Card emerged from Stealth Mode and became publicly available. It operates similarly to a traditional debit card.



"Central banks cannot afford to treat cyber currencies as toys – it is time to realise they are the real barbarians at the gate..."

Andrew Sheng, Chief Advisor China Banking Regulatory Commission

Brexit Spies and the Poker Game

Eyes, Ears, EUROPOL and Intelligence Sharing



Former Prime Minister David Cameron and current UK leader Theresa May

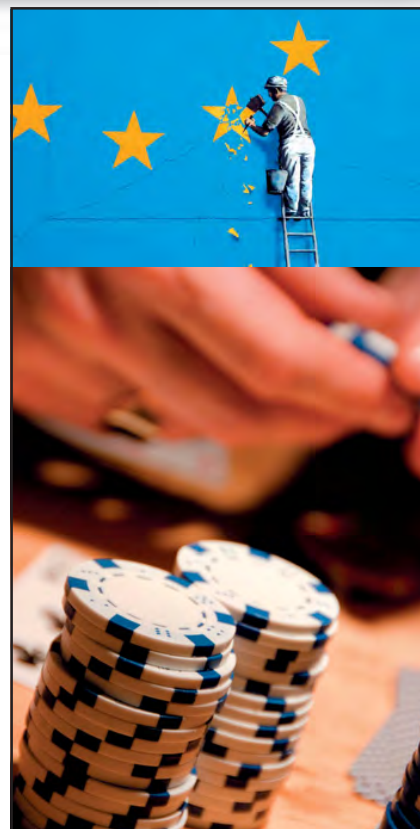


EU Commentators Claim British Brexit Advisors Using Powerful UK Intelligence Agencies as a 'Bargaining Chip'

Much debate rages on regarding Britain's role in intelligence collection and countering terrorism after it leaves the European Union. In the media, major EU-based newspapers and broadcasting agencies have continued to claim the UK will not be as secure due to new intelligence cooperation sharing measures which will need to be implemented. EU hardliners want Britain expelled with no gateway to security and intelligence channels. That's hardly likely as Britain provides more intelligence to sister agencies through its four major intelligence-collection agencies than any country in the EU. MI5, MI6, GCHQ and New Scotland Yard all contribute to European and world security, and it would be a major blow, not only to the European intelligence community in general, but EUROPOL, if restrictions and new rules of engagement are introduced following Brexit. Earlier this year, Prime Minister Theresa May

was accused of "blackmail" after stating Europe would be weakened if a "comprehensive security agreement was not agreed." One commentator said May and her team of Brexit negotiators were using British Intelligence as a "poker chip."

A great deal of focus is now on EUROPOL - the agency that started in 1998 and has grown in importance since 9/11. Its current Director is Briton Rob Wainwright, a former MI5 analyst who will probably be forced to step down when Brexit is completed. He is a great advocate of the current intelligence sharing programme, but has warned unless the UK negotiates what could be described as a status quo, then it could be damaging in respect of future security issues, especially in the theatre of counter-intelligence and all aspects of the war against terrorists. "I have seen how the threats of terrorism and organised crime have become more global





Rob Wainwright, EUROPOL

and the need for greater international police cooperation is absolutely essential to keep us safe," he said. Essentially, Mr Wainwright believes Britain's departure will leave it more exposed and vulnerable to terrorism and major organised crime unless it maintains some sort of presence.

UK INTELLIGENCE FEEDS

One man who has worked in the field of terrorism legislation and the mechanisms which support counter-measures is Lord Alex Carlile, a former independent reviewer of terrorism. He states Europe would be much poorer in respect of security if Britain is not a

major participant in this field. "The British police and the British intelligence services provide a disproportionate high amount of the information which helps the European intelligence agencies and police prevent and detect terrorism," he said. "They need us more than we need them." Mr Carlile believes it is "inconceivable" an agreement will not be reached.

EUROPOL's Wainwright insists that a deal is still possible and that the UK should negotiate with Brussels to ensure access remains open to collected intelligence and future security threats. "It is important for Britain to get this right. It's about the security of the country. Not just for Britain, but of Europe."

FIVE EYES SUSPICION

For years many European officials have argued that Britain has had a privileged status in respect of so-called 'Five Eyes' membership. The international module that exists between the USA, UK, New Zealand, Canada and Australia which sees huge amounts of intelligence flow to each country. Europe is not part of this agreement, and member states have accused the UK of failing to pass on materials. This is not the case of course, and a channel has always existed which directs information to relevant parties. Similarly, for decades EU states have accused the UK and USA in particular, of operations tantamount to industrial espionage and parliamentary



Lord Carlile

election monitoring. Some European commentators and intelligence watchers have already accused British Intelligence of passing classified information to the UK Brexit negotiators that provides a unique insight into European policy regarding the departure of Britain from the EU.

Despite the reservations and banter from both sides of the English Channel, few intelligence watchers believe Britain will depart the intelligence sharing mechanism in Europe, including EUROPOL. "A new agreement will need to be negotiated, but even the European Union recognises that the loss of high-grade intelligence from the UK would be utterly damaging," a senior intelligence specialist on European intelligence affairs and security told Eye Spy. "Europe would be much weaker without access to intelligence secured by MI6 and other UK agencies, therefore it's essential that Brussels keep liaising with Britain in this important field."



European Parliament Building, Brussels



Jean-Claude Juncker, President of European Commission. He believes Britain "will soon regret leaving the EU..."

THE

Spy Operations Revealed as Tensions Rise in Far East Theatre



Agencies such as MI6 and the CIA have long attempted to understand and determine from whence the technology was sourced by North Korea to build its nuclear warhead-carrying rockets and long range missiles. In the past decade, a number of nations, individuals and even companies (some government controlled) have been identified as being the likely culprits. MI6 too has monitored the comings and goings of scientists and couriers from several NK-friendly states, including Iran: here information is bought, exchanged and discussed. Indeed, some of Tehran's own nuclear secrets seem to correlate with that of Pyongyang, including rocketry, buildings and test stations.

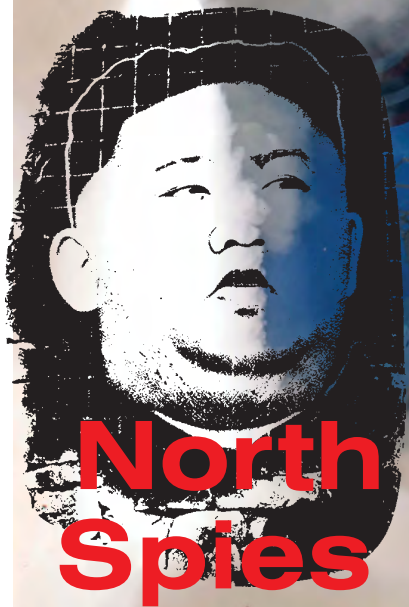
Now, following the successful launch of yet another North Korean inter-continental ballistic missile (ICBM) on 28 August, this time a Hwasong-12 over northern Japan, there is genuine worldwide concern that conflict is inevitable. ➤



UKRAINE

STING

June 2014. USS John Paul Jones launches a RIM-174 Standard ERAM (Standard Missile-6, SM-6) during a live-fire test of the ship's Aegis weapons system in the Pacific Ocean



North Korean Spies and the

MISSILE TECHNOLOGY MYSTERY



Imagery released to CNN by the SBU to diffuse speculation North Korea sourced its rocket and space technology from the Ukraine.

1. A North Korean spy photographs bogus blueprints as part of a carefully orchestrated sting operation to supply the Communist country with disinformation. **2.** The prison near Zhytomyr, Ukraine where two jailed NK spies were jailed in 2012. **3.** Spy X5 in prison. **4.** The cell where X5 is detained along with eight other inmates

Intelligence watchers note the timing of the launch was significant - the 107th anniversary of the annexation of Korea by Japan in 1907. The United States responded within hours, announcing the shooting down (interception test) of a medium-range ballistic missile (MRBM).

BACKGROUND

North Korea has recently threatened the US Pacific territory of Guam amidst reports it is set to test its sixth nuclear bomb. In July, two

missiles were launched with commentators believing they were capable of striking some parts of the United States. Scientists and defence analysts remain unsure if NK has managed to miniaturise a nuclear warhead capable of insertion into a viable carrier, but intelligence sources believe that it is only a matter of time. President Trump meanwhile, has said Pyongyang would face "fire and fury" if it continued to threaten American and allied interests. And though intelligence on many parts of the NK programme remain beyond the reach of agencies such as the CIA, questions

continue to be asked about how North Korea has progressed so far, so quickly.

SOURCING TECHNOLOGY

One country recently caught up in the technology mystery is the Ukraine. For decades an integral part of the Soviet Union, in more recent times it has been engaged in fierce conflict with its former Russian ally. However, increasingly some intelligence experts have focused on one of the Ukraine's most important rocket, satellite and missile builders. The Yuzhnoye Design Office was a component of the Soviet space and weapons programme with its roots beginning in the early 1950s. Based in the city of Dnipro, Yuzhnoye was referenced as a possible source for some NK technology used in its ICBM programme - a suggestion vigorously refuted by the Ukrainian Government.

On 14 August 2017, London-based International Institute of Strategic Studies (IISS) noted



Captain Hans Sholley, commanding officer of US Naval Base Guam (NBG)



Ukraine stamp 2002 featuring Mikhail Yangel, founder of Yuzhnoye and a leading missile designer



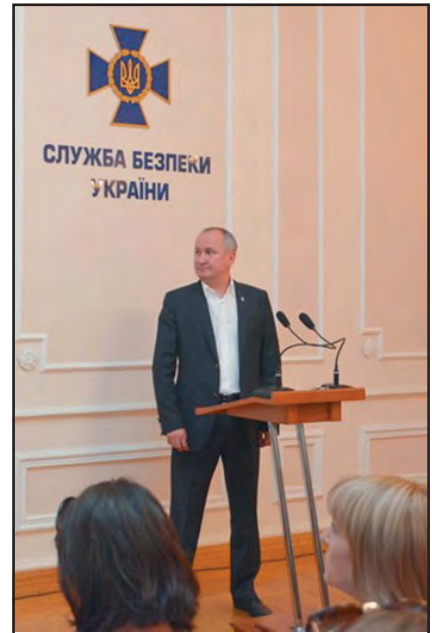
Yuzhnoye Design Office - General Designer Alexander Degtyarev and Mikhail Bondar Acting General Director and Chief Engineer

North Korea's 'technology leap' had been achieved with assistance from overseas parties. Few would argue against that point. The IISS report was compelling, detailed and very well researched: it focussed primarily on the rocket technology used in such programmes as Hwasong (and others). IISS argued that NK has '*acquired a high - performance liquid-propellant engine*' (combustion chambers and materials), from illicit networks in Russia and Ukraine. Other information also appears to have been

sourced in these countries - perhaps with covert assistance. And of course, the IISS also mentioned Yuzhnoye - that provoked the company to issue a lengthy and detailed response (see page 34). A company official dismissed the report as "bogus and not supported by facts."

SPIES AND BLUEPRINTS

All this commentary led to a debate about a little known espionage incident dating from



SBU Director Vasyl Hrytsak. Ukrainian Intelligence has dismissed reports North Korean spies sourced technology from the country's leading space and rocket technology company

around 2010 - and one which Ukrainian Intelligence was now keen to explain. In a surprising turn of events, Ukrainian officials released details of counter-espionage operations which targeted NK spies and diplomats. Indeed, the intensity of NK operations in the Ukraine grew to such a level

AEGIS BMD SYSTEM INTERCEPTS TARGET MISSILE



USS John Paul Jones

Just hours after North Korea launched its latest missile, America's Missile Defense Agency (MDA) and US Navy successfully conducted a complex missile defense flight test off the coast of Hawaii. This resulted in the intercept of a medium-range ballistic missile (MRBM) target using Standard Missile-6 (SM-6) guided missiles. The USS John Paul Jones detected and tracked the target missile launched from the Pacific Missile Range Facility on Kauai, Hawaii with its on-board AN/SPY-1 radar, and on-board SM-6 missiles executed the intercept.

MDA Director Lt. General Sam Greaves said: "We are working closely with the fleet to develop this important new capability, and this was a key milestone in giving our Aegis BMD ships an enhanced capability to defeat ballistic missiles in their terminal phase. We will continue developing ballistic missile defense technologies to stay ahead of the threat as it evolves."

This test, designated Flight Test Standard Missile-27 Event 2 (FTM-27 E2), marks the second time that an SM-6 missile has successfully intercepted a medium-range ballistic missile target.

Yuzhnoye State Design Office

Ukraine Space and Missile Technology Company Rejects Stories and Reports Linking it to North Korean Technology Leap



KIEV: On 16 August 2017, Yuzhnoye State Design Office (YSDO) issued a powerful rebuke of North Korean technology stories published by IISS and *New York Times*. The organisation said:

'They were fictional, false and inaccurate with regards to Ukrainian involvement. For

organisations such as IISS and NYT to publish such highly speculative material with unsupported claims and assumptions is unprofessional and inflammatory, with a seemingly political agenda.

'The material is riddled with technical inaccuracies, amateur level assessment of technology, and a clear lack of understanding of rocket and missile technology'.

YSDO then went on to lambast the authors and asked why no-one had sought clarity regarding the features. Officials at the company then meticulously listed comparative technology showing differences and stating that it was *'ludicrous to propose that the Ukrainian designs are present in North Korean systems'.*

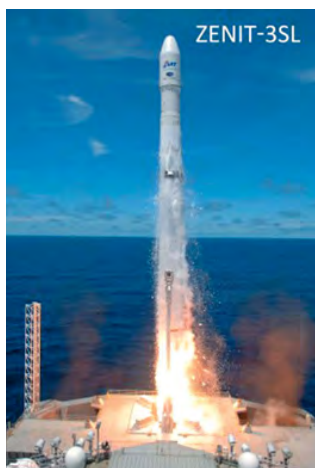
In a lengthy statement, YSDO concluded by stating that North

Korea received no help from the company whatsoever, and has formally offered to help determine who has provided assistance to North Korea. This offer of help was delivered to officials at the US Embassy in Kiev on 15 August.

The company ended (summarised) its indepth report

by saying: *'Yuzhnoye has always and will always be vigilant in non-proliferation efforts to keep technologies away from regimes that threaten world peace, irresponsible, inaccurate and false journalistic reporting won't alter this'.*

LINKS: www.yuzhnoye.com



that resulted in a diplomatic spat - Kiev barred all North Korean nationals from entering the country.

Of intelligence note and related to North Korea's hunt for technology, Kiev also released to CNN imagery secured by the Security Service of Ukraine (SBU). This showed a surveillance operation targeting three NK diplomats. On 27 July 2012, two of the Koreans were caught photographing classified documents. It transpired the counter-intelligence operation was actually a

'sting', almost certainly supported by two very well known foreign intelligence services. The Koreans had been liaising with men they believed were Ukrainian missile experts - but were in fact undercover SBU officers.

The documents were carefully created blueprints of missile technology - with a plethora of deliberate errors injected into the data. The Korean 'diplomats' had been tracked entering Ukraine after leaving their embassy in Moscow. At the men's trial in 2012, a list containing the information sought by the spies

was revealed. This included technology on ballistic missiles, systems, construction, spacecraft engines, solar batteries, fuel tanks, and other associated items.

Keen to dispel any suggestion that North Korean missile and rocket technology was sourced in the Ukraine, officials explained that one of the men was deported immediately, but two of the spies were given eight-year prison sentences - both remain in jail. CNN was given access to the operatives - known as X5 and X32. X5, thought to be aged around 55, told





THE NORTH KOREAN PROBLEM “Talking is not the answer...”

President Trump issued a chilling warning to North Korea

the news organisation he was born in Pyongyang and served as a trade representative in the North Korean Embassy in neighbouring Belarus.

Ukraine Deputy Minister of Justice, Denys Viktorovych Chernyshov, told CNN: “They (North Korea) have asked the Ukrainian authorities the men be extradited to continue [serving] their sentence in North Korea. But because they are being held for spying... we obviously denied their request.”

CNN also interviewed an SBU officer who worked on the 2012 sting operation. He said it was “impossible” that NK could have secured any Ukrainian rocket technology and “he was sure all espionage attempts had been intercepted.” Interestingly, he further stated



30 August 2017. Defense Secretary Jim Mattis met with South Korea’s Defense Minister Song Young-moo (inset) at the Pentagon to discuss possible responses to North Korea’s provocative action. Both parties believed a resolution would be secured though few details were released



Propaganda images released in August by North Korea

1. Kim Jong-un walks past a probable non-working solid-fuel rocket casing

2. & 3. Kim Jong-un pictured with officials and a number of large technical posters.

Analysts believe these show the new rockets Pukguksong 3 (not an ICBM) and a three-stage missile Hwasong 14



Britain's Prime Minister Theresa May met with Japan's Prime Minister Shinzo Abe in late August offering UK support to the country against North Korea aggression. Both countries agreed to strengthen military ties. During her three day visit, May visited Japan's flagship helicopter carrier the JS Izumo (pictured)

that five North Koreans were deported in 2015 for "assisting intelligence work in the Ukraine."

The last word on this fascinating spy drama must go to Mr Chernyshov. He said that because the spies were unsuccessful in their hunt for rocket and missile technology, "they can't expect much of a heroes welcome when they are released in September 2018 and return home."

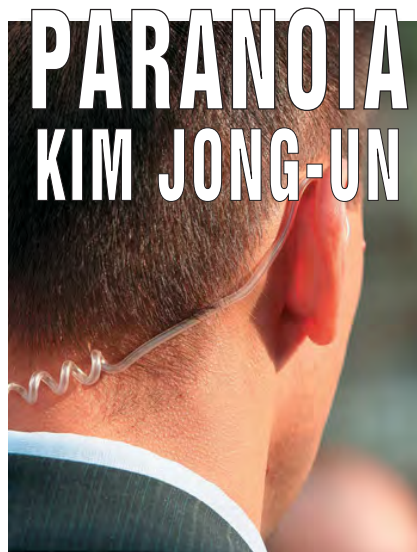
However, all of this leaves one burning question unanswered - as noted in the IISS report. What or whom has propelled the North Korean ICBM programme to such heights in the last two years? Ukraine officials believe they have the answer... the Russians - though Moscow rejected the allegation.



Ukraine Deputy Minister of Justice, Denys Viktorovych Chernyshov

International Institute for Strategic Studies IISS

The International Institute for Strategic Studies (IISS) is a world-leading authority on global security, political risk and military conflict. The IISS was founded in the UK in 1958 with a focus on nuclear deterrence and arms control. Today, it is also renowned for The Military Balance, its annual assessment of countries' armed forces and for its high-powered security summits, including the IISS Shangri-La.



NK Leader Hires Former FSB Personnel for Protection and Counter-Espionage

Amidst threats to his country and his person, the leader of North Korea is reportedly obsessed about his personal safety. Rumours abound in the Far East media that he now travels only at night using different cars, and at meal times has all his vegetables inspected by microscope for poisons. Increasingly paranoid, he orders every leaf of lettuce to be carefully inspected. The 'highest authorities' in the secretive country now closely check all vegetables grown on his own farm - called 6.17.

A source inside North Korea told colleagues: "Instead of just going through farm inspections, the produce needs to go all the way up through the Escort Bureau in order to receive the green light before being presented to the leader." In addition, only those with suitable 'songbun' - (family links and loyal to the reigning Communist party) - are allowed to work on the farm. Prior to this, "they have had to study to become doctors before becoming farmhands."

South Korean Intelligence believe his paranoia and his latest actions to increase tensions using the threat of war, could be linked to an assassi-

nation attempt which reportedly took place by his own disgruntled people in Pyongyang during a power struggle in 2013. He also believes the West has put together a 'decapitation force'. And now, according to journalists, he has hired former Russian FSB counter-terrorist officers to instruct his bodyguards on how to detect and respond to terrorist attacks.

Another NK source told *Asahi Shimbun*, Japan's leading newspaper, that Kim felt the KGB, the former Soviet Union's main security and spy agency, had decades of practice in defending high-value targets against attempts at regime change and were the agency of choice. It was reported the agents came to Pyongyang as military advisers to give advice to Kim's guards on how to handle threats. Some writers also speculated that the Russians could well be involved in a counter-espionage role targeting South Korean and US spies.

"North Korea is showing great interest in defending against assassination carried out by US-made state-of-the-art weapons," the source told *Asahi Shimbun*, according to a translation from United Press International. The former spies from the Soviet security agency were asked "to carry out military education and training needed in detecting and pre-emptively suppressing acts of terror."

The source also said Kim was particularly worried about advanced US weapons such as the Grey Eagle UAV scheduled to operate in South Korea in 2018.



Kim Jong-un



NK Nuclear Military Programme Advances with Hydrogen Bomb Detonation

MAIN: 28 August 2017 - Northern Japan. Marine Corps F-35B Lightning stealth fighters based at Air Station Iwakuni, Japan, fly alongside USAF B-1B Lancers and Japan Air Defence Force Koku Jietai F-15J fighters. **TOP:** US Navy Amphibious assault ship USS Wasp set sail for Sasebo, Japan on 30 August. The ship will assume duties as the forward-deployed flagship of the US 7th Fleet. **BOTTOM:** 31 August. A USAF B-1B Lancer prepares to receive fuel whilst flying from Anderson Air Force Base, Guam, into Japanese air space



POINT OF NO RETURN?

SUCCESSFUL NORTH KOREAN NUCLEAR TEST REVEALS EXTENT OF TECHNOLOGY PROGRESS

North Korea has claimed its sixth nuclear test, this time using a miniaturised hydrogen bomb for use on a long-range missile. Pyongyang says the detonation was "a perfect success." America responded by stating Kim Jong-un is "begging for war."

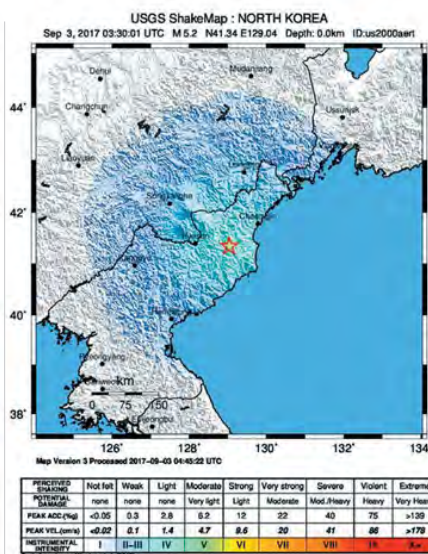
South Korean officials said the latest test took place in Kilju County on 3 September, where the North's Punggye-ri nuclear test site is

situated. Seismologic readings from the US Geological Survey show a tremor in the region measuring 5.6 magnitude with a depth of 10km (six miles). This was later upgraded to 6.4 magnitude at 0km.



Nuclear weapons expert Catherine Dill (left) said: "It was not yet clear exactly what [type] of nuclear weapon design was tested. But

based on the seismic signature, the yield of this test definitely is an order of magnitude higher than the yields of the previous tests." Experts now acknowledge a nuclear device was detonated - and have concluded the device was approximately five times bigger than that dropped on the Japanese city of Nagasaki in WWII.



3 September 2017. US Geological Survey Earthquake Hazards Programme 'shake map' showing the magnitude 6.3 intensity explosion-generated earthquake





South Korea - August 2017. US Marine Corps troops train with their counterparts from South Korea

USPACOM - OFFICIAL STATEMENT: US Pacific Command protects and defends, in concert with other US Government agencies, the territory of the United States, its people, and its interests. With allies and partners, PACOM is committed to enhancing stability in the Asia-Pacific region by promoting security cooperation, encouraging peaceful development, responding to contingencies, deterring aggression, and, when necessary, fighting to win. This approach is based on partnership, presence, and military readiness.



Han Tae-song

Initial reports of the test came hours after Pyongyang said it had miniaturised a hydrogen bomb for use on a long-range missile, and North Korean leader Kim Jong-un was pictured with what state media said was a new type of hydrogen bomb. Excited State media broadcasters said "the device could be loaded on to a ballistic missile." Defence

expert Melissa Hanham, of the Middlebury Institute for International Studies in California, said that the North's claims could not be verified from the photographs alone. *'We don't know if this thing is full of styrofoam, but yes, it is shaped like it has two devices'*, she wrote on Twitter. Hydrogen bombs detonate in two stages. *'The bottom line is that they probably are going to do a thermonuclear test in the future, we won't know if it's this object though'*, she added.

Intelligence analysts say the claims should be treated with caution, but acknowledge North Korea's nuclear capabilities are clearly advancing despite China's urging to "face up to the firm will" of the international community and the denuclearisation on the Korean peninsula.



North Korea's Ambassador to the United Nations in Geneva, Han Tae-song, said the recent tests were "self defence measures" and a "gift package addressed to the United States."



Kim Jong-un discusses the nuclear bomb project with scientists attached to the programme



INTERNATIONAL REACTION

A Chinese Foreign Ministry spokesman said of the test: "China's government expresses resolute opposition and strong condemnation toward this." Russia, meanwhile, said the test defied international law and urged all sides involved to hold talks, saying this was the only way to resolve the Korean peninsula's problems.

Director General of the International Atomic Energy Agency (IAEA), Yukiya Amano,



described the test as "an extremely regrettable act", which was "in complete disregard" of the demands of the international community.

US President Donald Trump tweeted: '*North Korea has conducted a major Nuclear Test. Their words and actions continue to be very hostile and dangerous to the United States. North Korea is a rogue nation which has become a great threat and embarrassment to China, which is trying to help but with little success*'. Defence chief James Mattis said any threat to the US or its allies would be "met with massive military force." US Ambassador to the United Nations Nikki Haley said her





“North Korea was begging for war...”

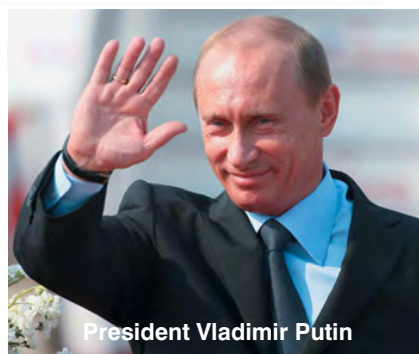
US Ambassador to the United Nations Nikki Haley



President Trump and Japanese Prime Minister Shinzo Abe

country did not want war but “patience was not unlimited.” However, she added North Korea was “begging for war.”

Russian President Vladimir Putin said threats of further sanctions against the Communist country were “useless.” He said North Korea would “rather eat grass than give up their



President Vladimir Putin

nuclear programme.” He called upon the international community to promote dialogue among all interested parties.

UK Foreign Secretary Boris Johnson described the test as “reckless and could represent a new order of threat.” He added that “all options are on the table.”

In a joint statement, German chancellor Angela Merkel and French president Emmanuel Macron branded the test a “new dimension of provocation” and said the EU and the UN Security Council must respond.

In the Middle East, the United Arab Emirates condemned the detonation. An official said it represents a “genuine threat to international security and stability.”

Despite sanctions and dire warnings from the international community, Kim Jong-un continues to ramp up tensions with the world.

Intelligence analysts believe the situation in North Korea has become dangerous - for any armed inter-action between the US and North Korea would destabilise the Far East, with China, Russia, South Korea and Japan all likely to become major players in any conflict.



USAF personnel train at Camp Rodriguez, South Korea

NORTH KOREA BITCOIN HACK

Cryptocurrency Unit Nets Kim Jong-un Millions

Intelligence cyber specialists report that North Korea appears to be stepping up efforts to secure bitcoin and other cryptocurrencies, which could circumnavigate trade restrictions including new sanctions approved by the United Nations Security Council.

Hackers reportedly attached to a secret NK Government (military) cyber element have been tracked engaging known cryptocurrency exchanges in South Korea and related sites, according to a new report from security research group FireEye Inc. “There is evidence to suggest the regime has successfully breached security walls and actually stolen

money,” one source said. FireEye said the NK probes began in 2016 and confirmed that bitcoin ‘wallets’ were compromised. One South Korean cryptocurrency exchange, Yapizon, announced in May that it was hacked and lost

3,816 bitcoins - \$5.3 million. The NK unit also breached an English-language bitcoin news website and collected bitcoin ransom payments from global victims of the malware WannaCry, according to researchers.



Jong-un’s interest in cryptocurrencies comes amid rising prices and popularity. The same factors that have driven their success. The FBI is but one of a number of agencies investigating the action, but its cyber specialists acknowledge that bitcoins are a useful fund raising and money laundering tool.

US and UK security officials admit North Korea has “embraced digital cash,” and the country’s interest in bitcoins will inevitably increase in future months as sanctions start to impact.



CYBER SUSPICION

KASPERSKY LOSES STATUS IN US AS APPROVED CYBER SECURITY PROVIDER

Suspensions surrounding Kaspersky Lab, the Russian cyber security and anti-virus provider, and its close ties to Russian intelligence agencies, has resulted in the firm being removed from two lists of approved vendors used by government agencies to purchase IT services and equipment. The government directive gave offices using Kaspersky security tools 30 days to remove all software. This follows a Senate Intelligence Committee meeting in May, when senior intelligence and defence officials were asked if they were comfortable with the Russian-manufactured software on their computer systems. Andrew McCabe, FBI Deputy Director (acting), said “no.” He was joined by CIA Director Mike Pompeo, National Intelligence Director (ODNI) Dan Coates and NSA Director Mike Rogers, to name just a few.

Earlier this year, FBI agents visited at least a dozen US employees of Kaspersky Lab at their homes as part of an investigation into its operations. According to a spokeswoman for the US General Services Administration (GSA), the decision to withdraw the company was made “after review and careful consideration.”

Kaspersky Lab has repeatedly rejected claims that the company has covert ties to the Kremlin and stated that “by all appearances,



Kaspersky Lab happened to be dragged into a geopolitical fight where each side is trying to use the company as a pawn in its game.”

Kaspersky released a statement regarding the US directive: ‘No credible evidence has been presented publicly by anyone or any organisation as the accusations are based on false allegations and inaccurate assumptions’. It went on to say it would ‘never help any government in the world perform espionage or cyber offensive efforts’.

The company’s founder and CEO Eugene Kaspersky, who once attended a KGB-



Eugene Kaspersky



Richard Burr, Chairman of the US Senate Select Committee on Intelligence

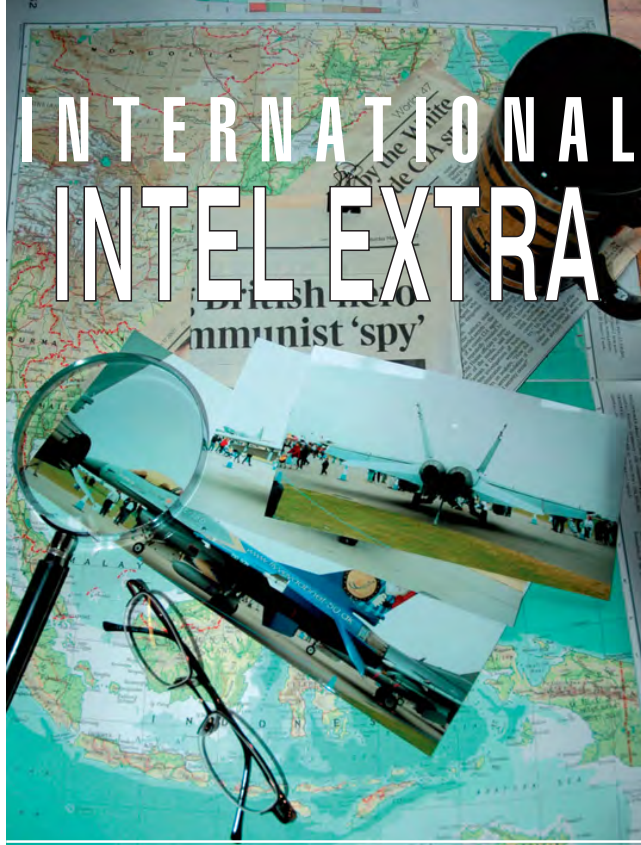
sponsored school and worked for Russia’s Defence Ministry even offered to testify before Congress and turn over the source code of his company’s products to US authorities. All to no avail.

Following the withdrawal and continued US government criticism, Best Buy, the largest US consumer electronics corporation, has confirmed that it will no longer sell the company’s products. A Best Buy official said “there were too many unanswered questions,” and that “technical staff could remove the Kaspersky software from users’ systems.”

Some 400 million people worldwide use Kaspersky security software.



INTERNATIONAL INTEL EXTRA



REVIEW • NEWS • DIGEST

INTERCEPT CONCERNS

Australian Intelligence (ASIS) Focus on China

Australia's Parliament is reportedly reviewing the use of cell phones built by the ZTE Corporation, a leading Chinese telecommunications equipment and systems company. The Telstra Tough T55 handset is available to Australian parliamentarians to purchase online through the Information, Communications and Technology (ICT) unit of the Department of Parliamentary Services (DST). The review follows information provided to the DST that members of the United States Congress and the House of Representatives' intelligence committee have expressed serious concerns about the ZTE Corporation in recent years regarding its links to

Chinese military [intelligence]. In addition, Australia is also concerned about China's Huawei Technologies, plans to provide



ASIS Director Nick Warner

SURVEILLANCE OVERSIGHT WATCHING THE WATCHERS

The Investigatory Powers Commission (IPC) has officially started operating in the UK and replaces the previous body called the Interception of Communications Commissioner's Office (IOCCO).

The IPC is an expanded oversight commission regulating the intelligence services and surveillance by various state agencies. The new office is staffed by approximately 70 people, including both current and

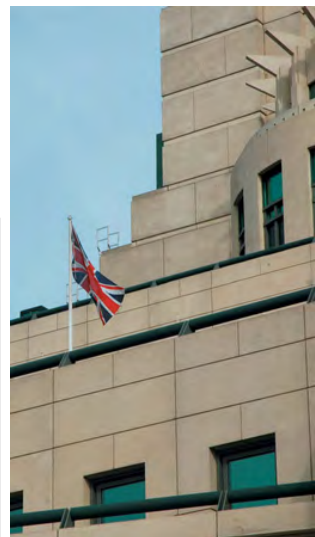


retired senior judges as well as inspectors, technical and legal advisers, and scientists on a technology advisory panel. The judges will counter-sign warrants for surveillance that are now only signed by politicians to check that the interception of phone calls, and the handling of agents, surveillance and powers permitting bulk collection of communications data are carried out within the law.

The IPC will monitor the UK's three primary intelligence agencies - GCHQ, MI5 and MI6, plus the National Crime Agency (NCA), police forces, the Serious Fraud Office (SFO), HM Revenue and Customs, local authorities, prisons and government departments as well as fire and ambulance services, the Gambling Commission, Ofcom, the NHS Business Services Authority and the Food Standards Agency.



Lord Justice Fulford



Its first commissioner and presiding judge, the Right Honourable Lord Justice Fulford, who has presided over a number of high-profile intelligence-related case files, including the 21/7 attempted London bombing trial, said: "From today, and for the first time, investigatory powers will be overseen by a single body applying a consistent, rigorous and independent inspection regime across public authorities. This is an important milestone as we start to implement the new oversight powers set out in the Investigatory Powers Act."

high-speed Internet to the Solomon Islands, a small Pacific island nation with which Australia shares Internet resources.

Intelligence agencies in the United Kingdom and the United States have issued warnings since 2011

that Huawei Technologies relied on a series of formal and informal contacts with the Chinese People's Liberation Army and the Ministry of State Security. The concern being that, by constructing the Solomon Islands undersea cable, Huawei would be "plugging into Australia's telecommunications infrastructure backbone," something that, according to one



Huawei Technology building in Shenzhen, China and ZTE cell phone



Solomon Islands Prime Minister Manasseh Sogavare with Australia's High Commissioner Andrew Byrne

intelligence official, "presents a fundamental security issue."

To complicate matters further are allegations that the Solomon Island Government contracted the services of Huawei after the Chinese company promised to make a multi-million dollar donation to the ruling political party. Attempts by the Director of the Australian Secret Intelligence

Service (ASIS), Nick Warner, to convince the country's Prime Minister, Manasseh Sogavare, to drop Huawei from the project have so far gone unheeded.

Sogavare said that his government would "continue to have discussions with the Australian Government to see how we can solve that security issue."

PORTUGAL SECRET SERVICE New Female Director Appointed

Portugal's Prime Minister Antonio Costa has announced the appointment of Maria da Graca Mira Gomes as head of the country's secret service - Sistema de Informações da República Portuguesa (SIRP - informations System of the Portuguese Republic). Gomes held the position of Portuguese Ambassador to the Organisation for Security and Cooperation in Europe (OSCE) in Vienna, and holds a degree in law from the Faculty of Humanities at the Catholic University of Lisbon, with a postgraduate degree in European studies.

Gomes' appointment follows her predecessor's warning that the country's secret services have "lost dignity and are obsolete," in respect of confronting threats to national security.

Prime Minister Costa said: "Ms Gomes possess extensive experience in policy-related issues, foreign and security policy and defence."

- SIRP oversees Portugal's two primary intelligence services - SIED (Defence and Information Service) and SIS (Security Intelligence Service).



Maria da Graca Mira Gomes with OSCE High Commissioner Lamberto Zannier



HACKER JAILED
CRACKAS:

Liverman
second from
left) outside
court

Justin Liverman, a 25-year-old member of the hacking group 'Crackas With Attitude' was sentenced to five years in prison after pleading guilty to conspiracy to hack US Government computer systems and accounts. Known under the online alias 'D3F4ULT', he was sentenced to the maximum allowed under the statute.

Liverman is one of five individuals facing charges for their connection to computer crimes committed by the group whose victims include more than ten US Government officials including former CIA Director John Brennan and former FBI Deputy Director Mark Giuliano. US prosecutors in the Eastern District Court of Virginia said: "Liverman conspired to attempt to intimidate and harass US officials and their families by gaining unauthorised access to victims' online accounts, among other things. Liverman publicly posted online documents and personal information unlawfully obtained from a victim's personal account; sent threatening text messages to the same victim's cell phone; and paid an unlawful 'phone bombing' service to call the victim repeatedly with a threatening message." Liverman will also be forced to pay \$145,000 in restitution.

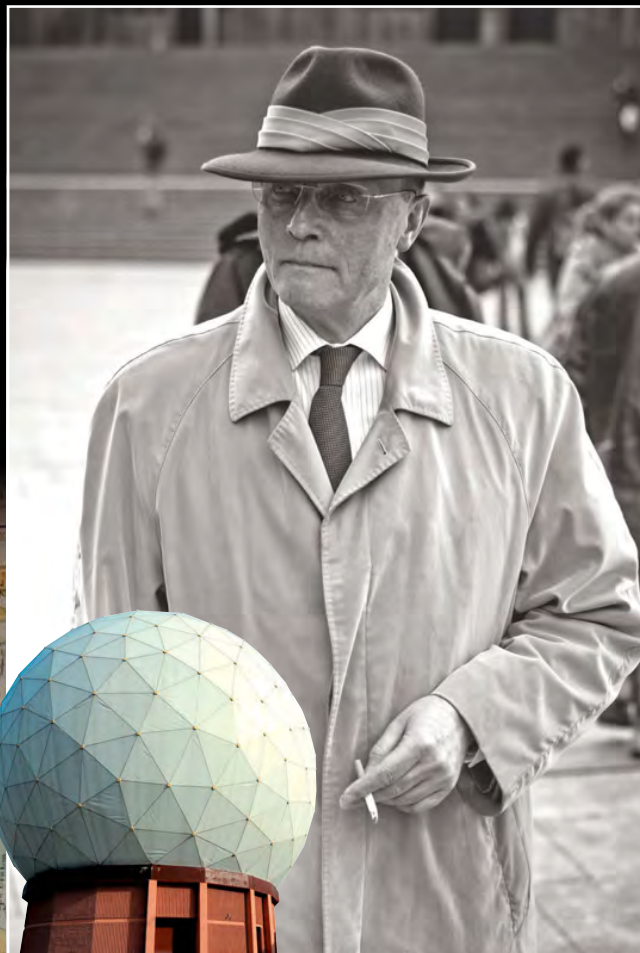
In court Liverman said: "I thought what I was doing was right in terms of political justice... but two years later, I realise I was completely wrong."

- The prosecution case against 'CRACKA', the leader of the group, is ongoing in the United Kingdom.

COURTESY: COURAGE

COURTESY: OSCE/JAKUB ROZSPAL

NOTES: COMMUNICATION & ESPIONAGE



Twenty five years ago - a decade before it became available publicly, software was created to 'catch' a key stroke electronically. However, if a physical device was not attached to the computer, then it meant an operative had to physically search a hidden programme to recover the data.

This all changed when users suddenly started to link their stand-alone computers to the Internet. Now there was a way to simply breach the security password and observe and remove files without anyone knowing. Other software could also be uploaded, including screen-grab technology. Such technology seeped into the public domain and programmes involving keystroke logging became common. Now software exists that can control internal computer cameras and engage microwaves effectively turning machines (and some smart televisions) into listening devices.



Eye Spy continues its journey examining the changing dynamics of spycraft

TRADECRAFT

PART 2

TRADING PLACES ADVENTURE IN TIME



Most people remain unfamiliar with the powerful multi-faceted and menacing cyber programmes that can cause mayhem in moments. An array of other entry methods into electronic devices exist and cell phone users are often warned about spyware. But most are oblivious or unaware of just how easy it is to hack into a system. Eye Spy is well aware of rogue programmes freely available that will turn just about any cell phone into a spy phone - making all calls to and from the unit available to a third party. It's one reason why today's intelligence operatives usually carry at least one additional unit and are warned to limit conversation.

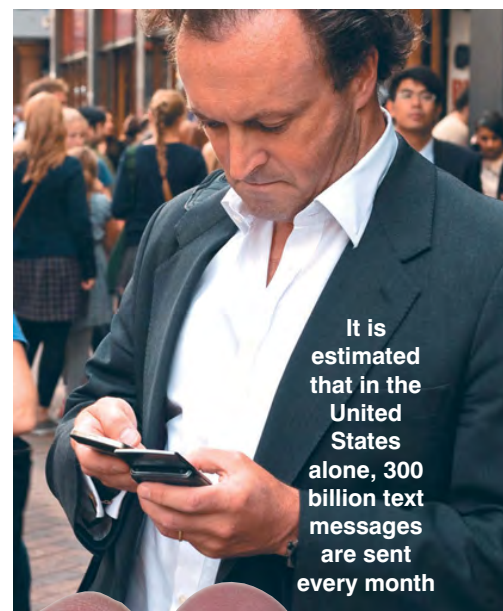
Whilst switching the SIM card may provide an additional level of security, there are spy programmes that upload software directly to

the machinery within the cell phone, thus circumnavigating the introduction of the new SIM. Current and emerging spy software is not limited to just to audible data, text messages and even imagery can now be sourced.

Fearing a security breach or a telephone bug, in years gone by a field operative would embark on a journey to a public phone box. But those days are long gone and probably in the next decade or so, the famous British public red telephone box will probably disappear forever. And in any event, communications where ever they are made or received, can now be challenged by machinery and methods labelled Black Box in the intelligence world. All of this is a far cry from what many hailed as the beginning of digital revolution with machines such as SIGSALY - the secure communication line used by Winston Churchill and President Roosevelt in WWII.

THE POWER OF INTERCEPTION

As a footnote and insight into how such technology has changed the spying game, especially in the field of communication, ten years ago the world's biggest and most powerful communications base, RAF Menwith Hill (NSA) in North Yorkshire, had the





A 2015 study by researchers at Nottingham Trent University, found that on average, a person will engage with their cell phone 85 times a day and spend up to five hours on electronic media platforms

Changing a SIM card affords some security, but if the unit has been infiltrated by advanced rogue (spy) software, it may not be sufficient to safeguard communications



proposal and provide a more tempting offer. It's an allegation never proven, but recent spy activities at the European Parliament and in London have only fuelled speculation.

PASSWORDS, PINS AND HACKERS

Though the dangers to ordinary members of the public are apparent, specialists warn we have done little to protect ourselves. Choosing a password to protect a piece of electronic media takes but a few seconds, but despite an array of security guidelines, and information available from a plethora of reputable outlets, most people opt for a simple word or series of numbers (birthdate for example) and stick with it. Amongst the top public security word used by cell and computer users? You've guessed it... PASSWORD. People for various reasons rarely change their passwords whilst most adopt a word or number that has some meaning or a simple combination. The same applies to PIN numbers on credit cards. Users will often select a birthyear or date embedded in their minds and stick with it. And just as relevant, the majority of computer users, including a whole host of businesses (including government bodies), do not use virus protection software.

The worlds of cyberspace and communication are not government or 'big brother' entities. Nor too is technology. Yet they are *the* growth area of espionage encompassing all its forms.

capability to track one million calls simultaneously. From here machinery would target selected numbers or listen for key words. The programmes that were once the envy of the world and relied heavily on lines used by British Telecommunications (BT), have been all but assigned to history. An intelligence and communications specialist told Eye Spy: "New technologies linked to the Agency's facilities in America have increased Menwith Hill's potential so much that watchers no longer comment on what it can or can't do." Coded speak which suggests don't compare.

Menwith Hill, since its inception in the late 1950s, has always been disliked by Britain's European neighbours, especially the Germans and French. On more than one occasion Brussels has claimed the base gives Britain and America a 'hidden advantage' in respect of securing business deals. In short, European ministers suspect that when negotiations take place and plans are drawn up to make a bid for a contract, the NSA and GCHQ secretly engage with competitors to try and learn their business plan. Henceforth US and UK contract companies can outbid or develop their



RAF Menwith Hill. The NSA station plays a vital role in the collection and dissemination of millions of communications, including many linked to espionage and terrorism



MI6 Chief Alex Younger with His Royal Highness The Prince of Wales



“Technology is behind everything we do”

MI6 Chief Alex Younger

A hundred years ago spies were often deposited in foreign enclaves by boat, or in wartime dropped by parachute. Some journey's took weeks and there was a good chance of failure. Now, armed with a reasonable computer, a fast broadband connection, off-the-shelf spy software and a little knowledge, it's possible to engage opponents in faraway lands without ever leaving the comfort of your home or office. Hackers are a damaging breed and some believe it's fun to 'turn the tables' on government systems. The number of security breaches reported by government agencies and concerns is growing every year. And while the hackers remain a mischievous bunch, those fearful of information loss are more concerned with the antics of government spy agencies or proxies.

Let's not fool ourselves into believing only agencies such as NSA, GCHQ, Mossad and the primary services have devoted cyber spy teams. Even Germany and France have established cyber units that trawl data from around the world - even targeting friendly nations.

COVER AND LEGEND

Yet the Internet is not all bad, and even old spy tradecraft has benefited. One area that often exposed agents and field operatives, especially 'new arrivals', was the creation of an unconvincing Legend or past history. By sourcing or providing a false background and life, agents could operate with the knowledge they had successfully adopted a new identity.



Few people opt to change their passwords, nor are those used often secure



An early tradecraft of those seeking a new identity (Cover and Legend) sometimes meant sourcing personal data from those who have passed away

Bogus work records (history) and a new family tree were paramount. Birth certificates could be altered and secreted in their respective place, so too death certificates of loved ones - just in case an adversary became suspicious. Training for an operation using a new Legend was difficult, so too the endless briefs about relatives' names, locations, events and even hobbies. All of this was manufactured in an environment that was intense. Failure or a lapse of concentration could lead to exposure. Russian Intelligence has a long history of successfully planting spies in foreign countries using Cover and Legend, and its illegals programme (see Eye Spy 110), has operated for decades. The starting point of a journey into the unknown once began with the sourcing of a new identity, and splore is littered with case files whereby data was secured from a gravestone, birth ➤



**INTEL
INSIDE**

Offutt AFB, Nebraska. Civilian and military personnel assigned to the 55th Strategic Communications Squadron pictured near two defence satellites. The organisation works with the Defense Satellite Communications Systems (DSCS) to provide secure command and control, voice, and data hotline capabilities worldwide including the US President, Secretary of Defense, United States Strategic Command (SAC), Joint Chiefs of Staff, Air Combat Command and numerous other organisations

certificate or better still, with help from a friendly official at offices handling births and deaths. Today, records relating to such matters are generally recorded electronically, and much past historical data has been removed from archives and also entered into more searchable machinery.

It's interesting to note therefore, that the Internet is now being used to assist in this tradecraft. From developing and creating false company work records, tax payments, banking receipts to journey's abroad, addresses and make-believe friends on social media platforms such as Facebook, the new Legend can become far more convincing. It can be further enhanced by stories and on-line

transaction details and even photographs showing the operative at a specific time and a place, for example on holiday or university. And given the role is being supported by covert agencies within government, further opportunities exist to project spies into a totally new person.

Whilst the methods of communication made famous by legendary spies will forever be embedded in the pages of history, today's operatives are a very different group. Yet all have two things in common - they must remain faceless to the outside world and at some point in their career they will engage with technology. However, the latter category today poses more danger. From exposure



Many citizens seem oblivious to the dangers of uploading huge amounts of personal data, including that of family and friends on social websites

following a cyber attack, as evidenced recently when the CIA was forced to recall some members posted overseas, to those in the field actually using communication devices: the 2006 MI6 affair involving a 'spy rock' device in a Moscow park for example. Technology and a service's increased dependence on it, is as dangerous to a field agent as a spycatcher engaged in counter-intelligence.

MI6 is but one of numerous organisations becoming ever more reliant on technology. Indeed, it freely admits on its website that: *'Technology's behind everything we do'*. As noted in Eye Spy 100, its modern website reflects a changing intelligence world. Whilst this may well be the case, some would argue it would be dangerous to leave behind and forget about the old tradecraft developed by past masters of espionage and subterfuge. And there is genuine belief in some quarters that old methods actually afforded more protection. Indeed, for all the modern communication methods available to today's intelligence collectors, most would agree, that sometimes it is best to trust in historical tradecraft, whether this is sending a simple letter or postcard, or passing information verbally.

The challenges faced by those operating in today's intelligence services may be a world apart from their predecessors, but by combining old tradecraft methods with new, this does provide a hidden advantage; especially in the field of communication, information delivery, concealment and security.

Eye Spy's *Adventure in Time: Communications and Espionage* concludes next issue, with a look at a variety of methods used to communicate and pass information, some definitely falling in to the bizarre category.



Whilst data collection has become far easier due to the methods available to the security services, the sheer number of cell phone calls, text messages and other forms of communication, has in itself caused massive problems for intelligence analysts. 'Overwhelmed' is a word that comes to mind



INTELLIGENCE FOCUS

ISIS FALLING DOWN

An overview of recent events, actions and opinion as the terrorist group continues to lose ground in the Syrian and Iraqi theatres



20-MINUTE TIMER AIRLINER BOUND FOR MIDDLE EAST FROM AUSTRALIA TARGETED

Security services from a number of countries derailed a complex two-part ISIS operation to bring down a commercial airliner and release poisonous gases on public transport.

A senior ISIS contact man shipped partially assembled components of a bomb, including

high military-grade explosive, on a commercial cargo plane flying from Turkey to Australia. Here it was assembled into a functional explosive device. The plan, involving three Lebanese-born brothers living in Australia and supportive of the terror group, was to place the device on an passenger aeroplane bound for the Middle East.

News of the attempted plot followed intelligence warnings that ISIS has embarked upon a programme to create viable bomb devices



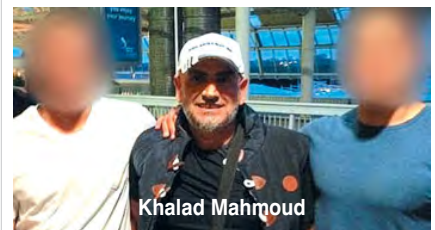
Amer Khayat attracted the attention of authorities by his constant excuse of entering Lebanon as "getting married"

using ordinary items - including electronic media platforms, for use in airline attacks.

THE JOURNEY

The operation unravelled following the actions of Amer Khayat. He came under the scrutiny of the intelligence services in both Lebanon and Australia after repeatedly travelling to his hometown close to the Syrian border. The man told officials he was getting married, but this reason was recorded on multiple occasions, thus alerting watching security officials. When he tried to board a flight again at Sydney Airport on 15 July, Khayat's luggage was found to be around 15 pounds overweight at check-in. Authorities later discovered an IED inside a meat grinder (and reportedly a 'barbie doll' containing similar explosives). Some reports suggest he reportedly left the case with one of his brothers and continued on the flight.

The plan was to bring down the aircraft (carrying 400 passengers and crew) approximately 20 minutes into its flight near Dubbo or Gilandra in central New South Wales. ➤



Khalad Mahmoud





Australian Signals Directorate - one of the intelligence agencies involved with intercepting terrorist communications



Mahmoud Khayat

have detected the IEDs. It later transpired Amer was seemingly oblivious that a bomb had been placed in his luggage. He remains abroad and there are no plans to issue an international arrest warrant. However, that's not how officials in Lebanon view the situation. The country's Interior Minister, Nouhad Machnouk said their operation began a year ago and Amer was a prime suspect. And despite Australian police saying "Amer had no idea he was carrying a bomb," Mr Machnouk said he had been arrested and was "fully involved in the operation."

THE TOXIC GAS PLOT

Australian security services discovered a second plan, involving building a chemical dispersion (hydrogen sulfide) device to release on public transport. Officials state the plot was

in its infancy when Australian police swooped and raided five residences across Sydney on 29 July. It is understood Lebanese security forces played a role in the investigation that triggered the operations - possibly related to information supplied by Amer. Prime Minister Malcolm Turnbull said the operations were "counter-terrorist related" and that the security services "foiled a plot to bring down an aeroplane in Australia."

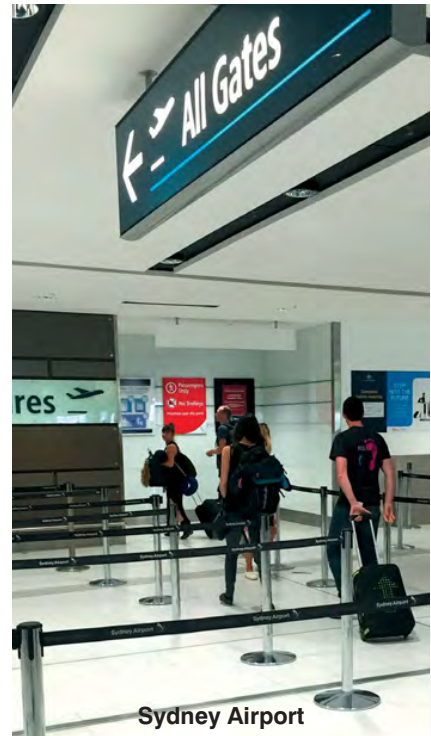
In Australia, Amer's brothers Khaled, 49 and Mahmoud, 32, have been charged with planning or preparing a terrorist act - both are connected to the airline and gas plots. The men will appear in court again in November, when further evidence will be produced. Another man arrested in the Sydney raids, Khaled Merhi, 39, has denied any involvement in the plots.



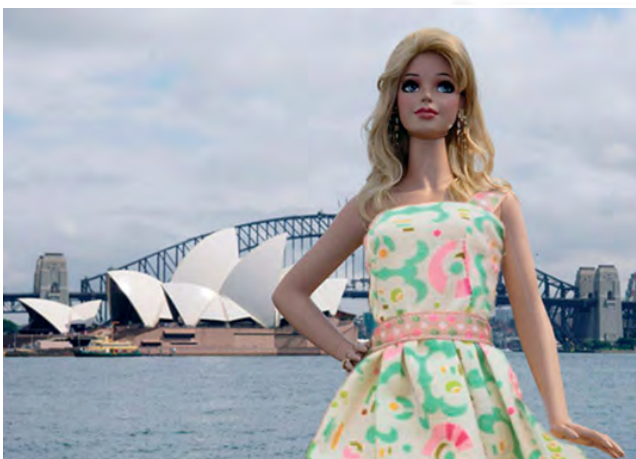
Prime Minister Malcolm Turnbull



A suspect is arrested following five simultaneous police raids in Sydney



Sydney Airport



Intelligence sources in Sydney are adamant explosives were also concealed in a 'barbie doll'



Australian Federal Police Deputy Commissioner National Security Michael Phelen

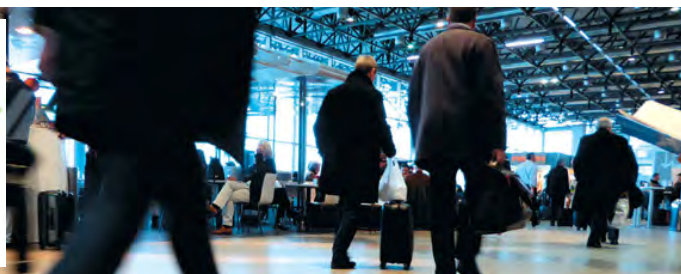


**Lebanon Interior
Minister
Nouhad Machnouk**

In Lebanon, Nouhad Machnouk, told a Saudi Arabia-owned TV channel that the four Lebanese-Australian brothers were all connected to the attack. As for Amer Khayat, intelligence sources in Lebanon believe he has imparted detailed information on the plots, including the secondary IED, built using a 'barbie doll'. This was in the event of the initial bomb-carrying device failing.

INTERCEPTED COMMUNICATIONS

Eye Spy believes the Australian Intelligence (Australian Signals Directorate - ASD) had worked with NSA and GCHQ after messages were intercepted from a suspected ISIS



operative who was providing guidance to the brothers.

The intercepts (initially e-mails) began in April 2017, around the time the airline plot was first discussed. Of much concern to the authorities in Australia (and elsewhere), is how the bomb components and explosives could have reached the country using an ordinary mail delivery service. This aspect is being further explored.

A fourth brother and alleged fellow conspirator, Tarek Khayat, described by Lebanese Intelligence as "the plot mastermind," and a "commander in ISIS" is thought to be still in Raqqa.

AUSTRALIA IN FOCUS

Australian intelligence and security services have successfully thwarted around a dozen

ISIS-inspired plots since the country's threat level system was raised in September 2014 to 'Probable'. However, five attacks have occurred. Seventy people in total have been charged in connection with 30 counter-terrorist operations performed by various forces.

CERTAIN

EXPECTED

PROBABLE

POSSIBLE

NOT EXPECTED

• Since 2014, the Australian Threat Level Advisory System has not been raised higher than Probable.

NIGHT ATTACKS LONDON AND BRUSSELS

On 25 August, a 26-year-old ISIS-supportive man from Luton, named as Mohiussunnath Chowdhury attacked police officers on the Mall outside Buckingham Palace, London.

As he drove in a menacing fashion towards a police van in a restricted area, he was confronted by unarmed officers. He then reached for a 4ft samurai sword concealed in the passenger footwell shouting "Allahu Akbar." Officers subdued the attacker, but three persons were injured in the incident.

MI5 engaged in the subsequent investigation and a few days later New Scotland Yard Counter Terrorism Command officers detained a second man in connection with the incident.



The Mall



Police at the scene of the Buckingham Palace incident

The men are being held under the Terrorism Act.

In court, it was revealed MI5 had discovered a note written by Chowdhury to his sister which read: *'The Queen and all her soldiers will all be in hellfire, they go to war with Muslims around the world and kill them without mercy'*.

ANOTHER ISIS ATTACK IN BELGIUM

In Brussels, another lone wolf operative attacked patrolling Belgian soldiers in Brussels. An official at the country's Federal Prosecutor's Office said the man raced towards the troopers with a knife shouting "Allahu Akbar." A trooper immediately shot the attacker who later died in hospital. The Belgian



man is of Somali origin and aged around 30. Few details have been released due to ongoing investigations, but like the London incident, it is being treated as terrorism. ISIS claimed responsibility via its media arm - Amaq 'News Agency'.



Troops patrol Brussels

REGRETFUL? THE GERMAN ISIS BRIDE

German legal officials are negotiating with their counterparts in Iraq to try and secure the release of captured ISIS operative and German national Linda Wenzel, 16. Criminal proceedings have been against the young woman who was pulled from a destroyed ISIS safehouse in Mosul, July, after Alliance fighters had eliminated a terror cell hiding in the building. Iraq judiciary officials want Wenzel, who says she regrets joining the terror group and just "wants to go home," to be tried in court over her actions.

Wenzel left her home in Pulsnitz, Germany and reached Syria via Turkey last year. She duly married a Chechen ISIS fighter who she met on an Internet chat site. Wenzel's father,



A tearful Linda Wenzel is led away by Iraqi troops following her capture

COURTESY: COUNTER-TERRORISM SERVICE OF IRAQ



Iraqi troops celebrate the defeat of ISIS in Mosul, but the destruction in the city is considerable and evident in this photograph



Reiner said: "I collapsed when I learned that Linda was alive."

According to informed sources in Iraq, Wenzel was deployed to roam about the city as part of an ISIS Morals Police unit - enforcing strict dress code for women. Several recorded

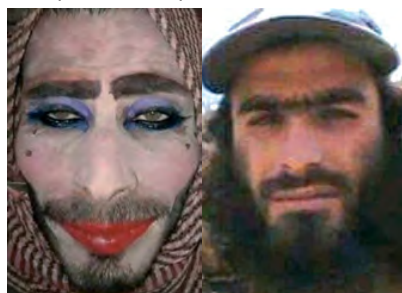
instances of punishment are known to have taken place, including executions.

Trying to secure her freedom may prove difficult. The Alliance unit found Wenzel, with a bullet wound in her leg, laying next to her dead husband with a gun in her hand. Iraq Intelligence also have a supposed statement from her that she acted as a sniper and "killed a number of troops during the retake operation," said one officer. Whilst operating for ISIS she used the name Umm Mariam.

If found guilty, Wenzel could be executed over her registration with ISIS and her alleged admission. However, this could not take place until she has reached the age of 22 under Iraq law, allowing German officials time to secure her release.

DISGUISES ISIS FIGHTERS EXIT

Dozens of ISIS fighters attempting to flee cities and former strongholds in Syria and Iraq have been captured disguised as women. Imagery released by the Iraq Army, particularly following successful operations in Mosul, show fighters wearing make-up and donning female clothing in an attempt to avoid capture.



INTELLIGENCE STAGGERING STATISTICS

Officials attached to Operation Inherent Resolve released details of a September Alliance operation targeting vehicles carrying ISIS fighters, tanks and munitions in the Syrian Desert between Humayma and As Sukhnah. Further statistics were also released. Alliance organisations from 72 nations fighting ISIS have retaken 50,000 square miles of territory held by ISIS in Syria and Iraq since 2014; some 5.5 million civilians have been freed from ISIS control;

115,000 Iraq Security Forces (ISF) have been trained and 11,000 specially vetted anti-ISIS operatives in Syria. In total, 26,000 counter-ISIS operations have been conducted. And whilst no accurate or tabled figure exists in respect of casualties, some intelligence sources believe as many as 100,000 ISIS-supportive operatives have been killed.

In respect of all deaths recorded by various civilian groups, the figure is believed to be approaching 500,000. British-based Syrian Observatory for Human Rights said 465,000 people have been killed or reported missing in Syria alone since fighting began in 2011.



Peshmerga troops near Mosul

SHRINKING CAPITAL

ALLIANCE EYES ON RAQQA



US-backed Alliance forces have retaken the Old City of Raqqa from ISIS. Hundreds of ISIS fighters died in a major offensive which began in June - thus further weakening the terror group's control in



Colonel Ryan Dillon



Various forces are involved in the operation to retake Raqqa

its self-proclaimed capital. US Army spokesman Colonel Ryan Dillon (Operation Inherent Resolve) said whilst the action represents a "significant step in the operation to take full control of the city," much fighting lies ahead. "This is still not over... but we are making progress," he said.

Kurdish and Arab forces have been engaged in street fighting for months, pushing ISIS forces into tiny enclaves. It is known both US and British Special Forces are involved in providing guidance and support.

The primary target in Raqqa are former government buildings known as the 'Security Block'. Here ISIS has built numerous defensive points and prepared a plethora of landmines and IEDs. Similarly, dozens of fighters have been selected to perform suicide missions. "This is of particular concern for Iraq forces," said one commander.

Some 25,000 civilians still remain in the city, many are being used to act as 'defensive shields' by approximately 2000-2,500 remaining fanatical ISIS fighters.

RUSSIAN ATTACKS

ENDGAME IN DEIR EZ-ZOR

Throughout August and September Russian bombers, helicopter gunships and warships launched a major offensive against ISIS positions targeting a crucial supply line into the important Syrian city of Deir Ez-Zor. Russian Defence Ministry officials said cruise missiles had "severed the terrorist channel," allowing SAA (Syrian Arab Army) forces access into the city's outer limits. Deir Ez-Zor is the last stronghold of ISIS in the region and is being attacked from three positions.

One notable area the SAA reached is the besieged Deir Ez-Zor Air Base which has been



Colonel General Sergei Rudskoy



Hmeymim Air Base near Latakia

surrounded by ISIS forces since 2014. Syrian President Bashar al Assad called the commander of Brigade 137 to congratulate troops.



President Bashar al Assad with Russian commanders at Hmeymim Air Base near Latakia



One bombing raid made by Russia on 7 September is said to have killed two senior ISIS commanders - Gulmurod Khalimov and Abu Muhammad al-Shimali

Colonel General Sergei Rudskoy, speaking at a press briefing, said 50 areas in Syria have been targeted by Russian-backed forces resulting in the liberation of 1,700 square miles of territory previously controlled by ISIS. Rudskoy said its air force had performed 990 combat flights in August destroying 40 armoured vehicles, 106 converted vehicles (machinegun-carrying) and killed 800 ISIS terrorists.

Russian Intelligence sources claim 25,000 ISIS fighters have been killed, injured or captured during fighting in the country since Spring.

A-Z

The Language of Spies

Another collection of unusual, but authentic terms and phrases used by those who work in the 'grey' areas of intelligence, espionage and security

BAG MAN

Most intelligence agencies have an undisclosed account used for expenses, including funds allotted to pay bribes. Bribery remains a key element used to extract information from people unwilling to cooperate or hesitant to impart essential intelligence. In many cases, just the

threat of disclosure of certain unpalatable facts may convince a target to cooperate, but there are hard targets who require and demand 'reward'. Intelligence officials are reluctant, increasingly so, to simply fill in a form requesting funds for such transactions, thus in the case of some well known organisations, front companies exist whereby they will be tasked with paying a fee. The men and women who actually deliver the money are known as 'Bag Men', and whilst known to the controlling agency, are not on any intelligence payroll.

In extreme cases where it is essential to distance further an agency from a payment, a Bag Man may well employ the services of an unwitting third party to deliver cash.

BUMP

One would be forgiven if those unfamiliar with the language of spies linked the word 'Bump' to an assassin. Though more mundane, it is fully attributable to its real meaning in the English dictionary, but quite complex when examined in relation to those selected to perform the activity.

In the world of espionage, intelligence collection and other associated areas, making



contact with a person, especially one oblivious that they have been targeted, is not an easy task. Contact, making friends and building a relationship, be it in a leisure or business environment, must have a starting point. When an operator embarks on first contact, this could be in a cafe, bar, street or a place where the target is known to frequent. And it could begin with an actual bump (inadvertent body collision). Eye contact and an apology follows. Thereafter, the operator attempts to engage in conversation. It's a lengthy 'liaison project', which could take weeks and other 'coincidental' contact may follow in different locations, with the line "well, what a surprise... we meet again." All such conversations are friendly. The endeavour has naturally been linked to honeytrap situations.





BURNED

An American and British description of a person (or operation), which has fallen foul to compromise. Agent exposure is the biggest fear of those charged with collecting intelligence. And whilst in more damaging cases, this could lead to arrest, prison or even execution and assassination of operators, it is generally spoken to describe the ending of an endeavour or the usefulness of a spy.

If an intelligence agency suspects an overseas operator (with official cover) has been identified, he or she will be designated as being 'Burned'. Once this happens, in most cases, the individual will exit the host country by conventional methods. It is damaging, for their role in covert operations exposed, means future assignments will be restricted to friendlier nations - for their identity will be



circulated amongst adversaries. For those operating with non-official cover, or as agents, the damage is considerable. Early detection of a Burned person may enable the handler to launch an exfiltration operation. Either way, damage is inevitable, and it may not always be possible to insert a replacement.



EXPIRED

Every agent or spy fears this designation (for various reasons including monetary). When an intelligence service embarks upon an operation, the biggest concern is exposure, especially to those involved in activities in foreign lands. The term 'Expired' or 'Expire' also reflects the usefulness of a contact or agent-in-place. In some darker areas of intelligence, case examples exist whereby an individual will be eliminated to remove all trace evidence of a controlling agency or operation.



Generally, however, it means the closure of an activity once the objective has been achieved, or the ending of an association with an individual who has served their purpose. It should not be confused with exfiltration, though some intelligence writers have used the term in this context.

MAIN LINE

The primary thread (direction) of planning, objective, implementation and outcome of an intelligence operation. A 'Main Line' is discussed and created prior to an operation with much

emphasis on avoiding distraction and trying to keep operatives' focus almost entirely on success. The challenge is to follow the Main Line and not deviate. This in itself is an admission that at any stage the operation is vulnerable and susceptible to outside interference, thus secondary (back-up plans) routes known as 'Branch Lines', may well have to be followed. In this regard, Branch Lines are effectively 'fall back' plans or additions which will help keep the operation (Main Line) on schedule.

Eye Spy is aware that another use of a Branch Line is one linked to deception, in this case all manner of ruses are created to deflect attention away from the Main Line (operation). Distraction, misdirection, disinformation and even illusion are elements used in Branch Line operations.

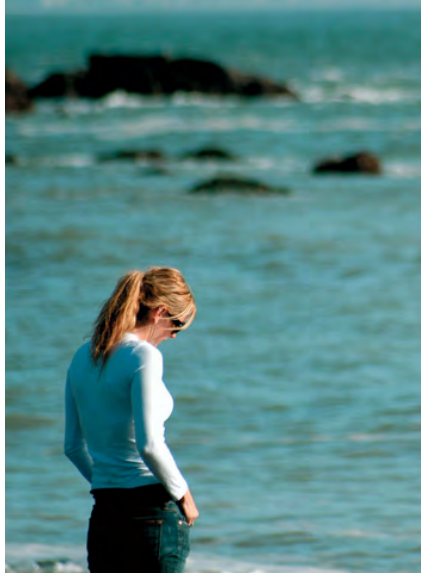
Perhaps a good analogy of a Main Line and Branch Line is the D-Day landings. In this case the objective was invasion, with other distraction operations engaged (even prior to invasion).



OFF GRID

Control and direction of any intelligence operation usually falls to those with experience or knowledge of a specific field, or individuals charged with completing a task (objective). Complex operations usually involve all manner of employees, support staff, technicians, and at the leading edge - spies, agents, contact people, handlers and field officers. At all times each 'person component' must remain aware and focussed on the task in hand. At any stage a lapse in concentration or a failure in one area could impact or totally derail an operation.

To maintain and support an operation, an agency will task managers (and operators), to be watchful of all those engaged. The term 'Off Grid', in this case, could apply to an individual or part of the operation which is out-of-step with the general mission.



In counter-intelligence work, the term is also frequently used to describe, for example, a 'person of interest' who has been under surveillance and has now simply disappeared. Similarly, it is used to describe an operator, agent or spy who has vanished without reason or apparent cause. When this happens, intelligence managers must quickly access the situation and plot a course of action, which sometimes means disabling (postponing) or ending an operation due to the real fear of wider compromise. Inevitably, it may mean that associates known to the individual are withdrawn.

OFF RESERVATION

A US Intelligence term which has been adopted by many organisations, especially attributable to agents engaged in overseas field work who may find it necessary to converse or illegally act with known adversaries. Such role play is dangerous, even more so when the actions of the operator appear 'out of sync' with instructions

or objectives (an agent may appear to perform an unauthorised mission, for example). The primary fear of any intelligence agency is an agent or officer 'out of control': the reasons could of course be plentiful, including ethical, mental health, alcohol or drugs abuse, being turned, going rogue or even having family members threatened.

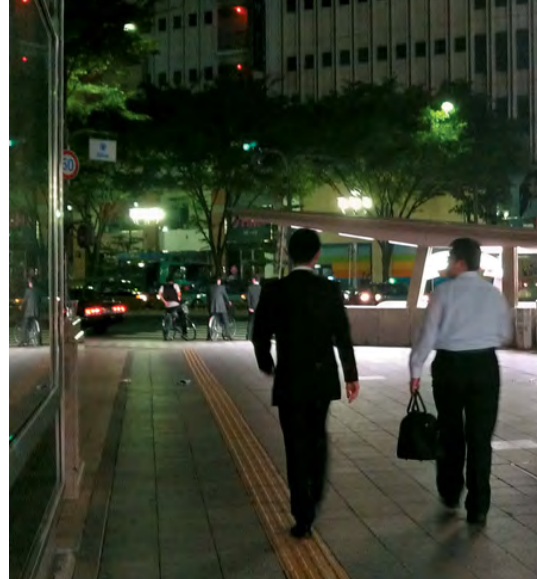
Once an operative has been deemed to go 'Off Reservation', careful consideration follows, and could lead to the withdrawal of the operator or closure of an activity.

The term is prevalent in all intelligence work (including some Special Forces operations), where a 'team' member fails to engage with instructions, or appears at odds with colleagues or questions the legitimacy of an act or objective.

PAROLES

Engaging or participating in an intelligence collection endeavour sometimes requires the collaboration of several agencies, including at times, friendly foreign services. Not knowing the identity of participants can cause embarrassment, a conflict of interests, or worse still - compromise and exposure. In the early stages of WWII, for example, there are instances when foreign-based MI6 officers operated in the same location as SOE agents - both entities oblivious to the other. And historical archive files reflect tensions and disagreements.

Today, the CIA and MI6 often find themselves delving into areas which could involve agent



placement. When this happens, due to the close cooperation that exists between the services, a plan of operations is agreed upon, saving time, monies and manpower. The Berlin spy tunnel is a good example (Operation Gold). However, occasionally it is necessary for both agencies to manoeuvre agents and 'contact' people into areas of interest. In most cases the identity of operatives will be made known to each other... but not always. Thus key words, known as 'Paroles' will be issued allowing for agent identification.

The reverse or downside to Paroles is compromise. If a key word becomes known to an adversary, all manner of problems may ensue, including capture, prison or worse. In recent months, several reported incidents involving a number of Chinese-based (alleged) CIA contacts have been captured, and at least one executed. Some intelligence watchers believe they used Paroles to communicate.

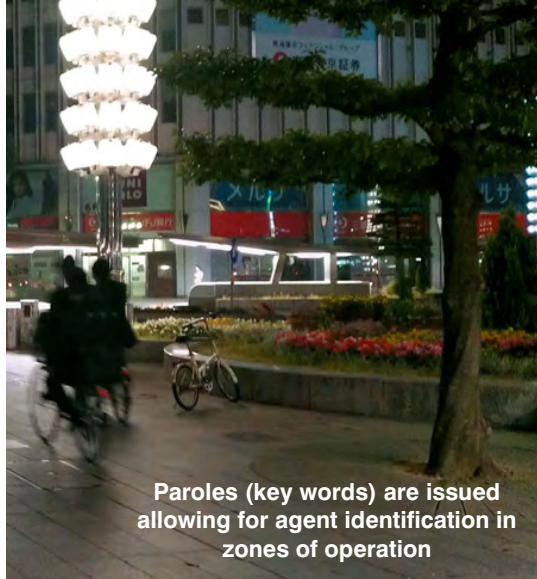
PLAYBACK

A term probably originating from World War Two, where spies from an adversary were captured and forced to continue corresponding/communicating with their controller. Though many case examples are known, it is recognised that hundreds more exist that remain undetected. These are regarded as particularly worrisome to an agency, for the information received from an agent could be tarnished or simply disinformation. When radio was used by a spy to pass information from an enemy location, to warn controllers that they had been captured and comprised, key words or terminology would be 'injected' in the transmission (or letter). More guarded counter-intelligence services would be able to determine if a captured spy was deliberately passing clues concerning his capture.

Nevertheless, forcing a spy to continue communication was an invaluable ruse, and



A concern for any intelligence agency or military command, is when an operative has been judged to go 'Off Reservation'



Paroles (key words) are issued allowing for agent identification in zones of operation

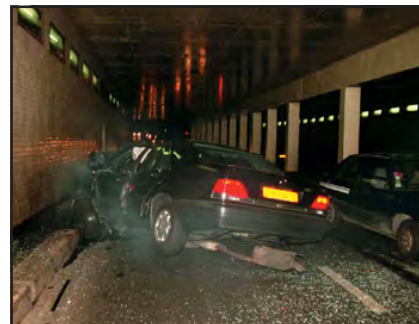
there are a plethora of 'Playback' stories, including several from the Cold War period. Indeed, today this intelligence element is applicable to exchanges made via the Internet, and in some case files, an agency will deliberately hack an account and inject false information. Once recognised by the end user, the role of an active or suspected agent is useless, and they may be withdrawn. Playback is a multi-faceted subject that has evolved over the years, and has threads to disinformation and a variety of subjects used to disrupt and confuse.



STAGECRAFT

Stagecraft should not be confused with [spy] Tradecraft or Theatre, for specialist operators involved with this highly dangerous element usually find themselves working outdoors and in vehicles.

Stagecraft is a term used to describe a deliberately staged car crash or accident, usually carried out when it is necessary to enhance an operation or distract attention away from another scene. In some cases it is performed to assist the safe removal of agents



or third parties from dangerous areas of operation, or block an exit route once a task has been performed. The objective is to 'deliver' a convincing accident, and one that is witnessed by third parties, thus allowing for 'enhancement'. Time is often a primary factor.

In some very dark areas the term has been associated with assassination. The death of the Princess of Wales in 1997, was controversially linked to Stagecraft. She died when a car driven by MI6 contact man Henri Paul, crashed in the Pont de l'Alma tunnel in Paris - this after being chased by journalists (the vehicle was also engaged in a close manoeuvre with another vehicle). A multitude of conspiracy theories still exist today, all involving a covert and intricate plot to kill Diana, all it must be said, are unproven. There are other more convincing case files linked to Stagecraft and intelligence.



Diana, Princess of Wales

Operatives who work in this field are not usually members of an intelligence service, but contracted from an associated agency. Most are skilled in surveillance.

STRAW MAN

In the world of intelligence, a 'Straw Man', sometimes referred to as a 'Straw Person', is generally recognised as an individual having no diplomatic cover who acts as a 'front person'. This could involve establishing a front company to conceal the activities of an intelligence-linked operation, or to represent the company in order that other intimate details, including names, remain concealed.

In more recent years, the term has been used to describe those working in any area of intelligence, who are likely to be sacked, killed, outed or are generally more vulnerable than others. ➤



EYE SPY

INTELLIGENCE MAGAZINE

SUBSCRIBE

A subscription will protect you
against any price increase

UK, USA, CANADA, EUROPE, ROW

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

UK 1 YEAR £29.95 ☐ USA 1 YEAR \$49.99 ☐ EUROPE/ROW 1 YEAR £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@eyespymag.com **ONLINE** www.eyespymag.com



**UNITED STATES OF
AMERICA**

Mail your subscription to:

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



UK, EUROPE, ROW

Send your subscription to:

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



CANADA

Send your subscription to:

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

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

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



ESPL 2017 UNIVERSAL EXPORTS 111/111/111

TRAVELLING MAN

For hundreds of years, perhaps thousands, information has been moved around the world by people. Adventure, pleasure, trade, business, learning and other activities mean that travel is essential. All afford opportunities to the world of intelligence and it is one area that remains as vital today as it did in the early days of the Roman Empire, for example, where great distances had to be travelled to impart a simple communication.

And despite the Internet (via satellite technology) enabling two parties to communicate in a micro second, there are occasions when it is necessary for an agent or intelligence officer to embark upon a journey. This of course means travel, but there are certain countries where suspicion abounds and it can be difficult for an intelligence service to operate or penetrate. Iran and North Korea are two examples. Nevertheless, having a genuine cause for travel can circumnavigate many obstacles, thus agencies such as MI6 still use operatives dubbed 'Travelling Men' (and Women). These could work in overseas trade, film or belong to the so-called Fourth Estate (media).

The use of such persons is dangerous, and one that naturally has caused mistrust. However, historically, there are numerous case examples whereby an actor, scientific explorer, student or anyone with a legitimate cause for travel, will either offer their services or be contacted to act as a Travelling Man to impart or receive information or make contact with an individual.



FAR BEYOND

REASONABLE DOUBT



ISRAEL STRIKES ROGUE SYRIAN WMD PLANT AS UNITED NATIONS REPORT CONCLUDES EVIDENCE PROVES CHEMICAL WEAPONS WERE USED BY ASSAD FORCES AGAINST CIVILIANS

SYRIA CHEMICAL WEAPONS

A United Nations Commission of Inquiry (COI) on Syria has officially accused President Bashar al-Assad's Government of carrying out over 20 chemical attacks since the start of the Syrian Civil War in 2011, including a sarin gas attack in Idlib province which killed 83 people (a third children) and injured around 300 others.

International investigators, provided with a plethora of intelligence and forensic data, including chemical burns' evidence, determined that an



A UN Commission press conference on the use of WMD by Assad loyalists



Su-22 fighter bomber, which is only operated by the Syrian Air Force (in the region), conducted four airstrikes in Khan Sheikhun on 4 April. At least one strike involved the dispersion of a chemical weapon.

Part of the damning report read: 'All available evidence led the Commission to conclude that there are reasonable grounds to believe Syrian forces dropped an aerial bomb dispersing sarin in Khan Sheikhun. ➤



Major General Yaakov Amidror



President Bashar al-Assad still has much support in Syria. He has denied allegations that his forces have used WMD

© IRA ABRAMOV



Major General Amos Yadlin, former Director of Israel's Amam speaking at a security conference in Munich, 2015

Perhaps more telling, physical evidence retrieved at the site: *'The Commission identified three of the bombs as likely OFAB-100-120 fragmentation bomb] and one as a chemical bomb. Photographs of weapon remnants depict a chemical aerial bomb of a type manufactured in the former Soviet Union'.*

UN investigators also stated Syrian Government forces had carried out chemical attacks on at least three other occasions since March in Idlib, Hamah and eastern Ghouta using weaponised chlorine.

ISRAEL STRIKES IN SYRIA

Just 24-hours after publication of the report, the Syrian Scientific Research Centre in the central province of Homs, believed to be

linked to the production of chemical weapons, was bombed on 7 September by Israeli Air Force jets killing two and causing major damage to the site. Major General Yaakov Amidror, a former national security advisor to Israeli Prime Minister Benjamin Netanyahu, said: "This is the first time that the target which was attacked was [identified] as a formal Syrian facility."

Major General Amos Yadlin, former Israeli intelligence chief of the Amam (Military Intelligence Directorate), said the raid sends three messages: "That Israel won't allow for empowerment and production of strategic arms. Israel intends to enforce its redlines despite the fact that the great powers are ignoring them. And that the presence of Russian air defense does not prevent airstrikes attributed to Israel."

A Syrian Army spokesman said the attack was "aggressive and threatened the general security of the region." He also warned there would be "repercussions."

INTELLIGENCE AND NORTH KOREA

In early September, a UN report confirmed that two North Korean shipments have been intercepted in the past six months enroute to Syria. Intelligence watchers link the materials to a contract made between the Korea Mining Developing Trading Corp. (KOMID) and Syria. KOMID is Pyongyang's primary exporter of prohibited chemical, missile engines and



A young Syrian boy sits atop an unexploded OFAB 100-120 high explosive fragmentation bomb

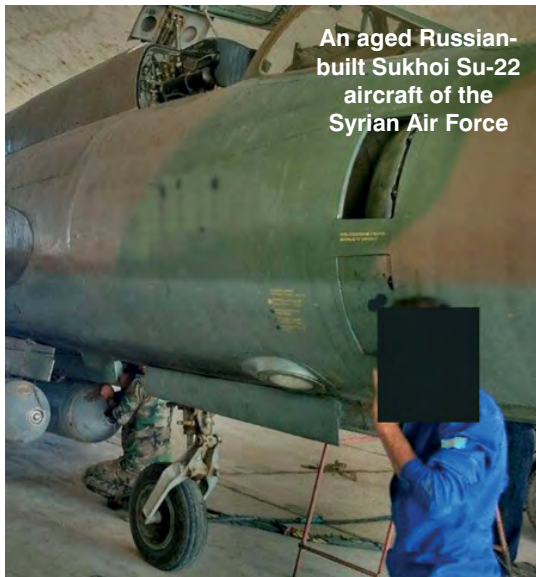
conventional arms. It was blacklisted by the UN Security Council in 2009 along with its two representatives based in Syria. According to security sources, North Korean engineers or technicians were employed at the Syrian



Syrians flee the site of an airstrike



A baby is freed by emergency service workers following an airstrike



An aged Russian-built Sukhoi Su-22 aircraft of the Syrian Air Force

strike Kim Jong-un via its liaison with underworld partners.

At the launch of the United Nations Commission of Inquiry (COI) report in Geneva, Paulo Sérgio Pinheiro, Chair of the UN Commission of Inquiry on Syria, said: "It underscores once

more how Syrian men, women, and children throughout the country remain the primary victims of violence perpetrated by the pro-Government forces, anti-Government armed groups, terrorist organisations and their affiliates."

SYRIA RESPONDS

Just a day or so after the release of the UN report, Syria's Permanent Representative at the Office of the UN in Geneva (ONOG), Ambassador Hussam Eddin Ala, sent a letter to the Commission, stating: 'Syria affirms that

CERS plant, which UN experts had reported as cooperating with KOMID in previous transfers of prohibited items.

Intelligence analysts suggest that as the UN report strongly suggests collaboration between Syria and North Korea in the development of prohibited weapons, the West and its allies have found a convenient way to



Chair of the UN Commission of Inquiry on Syria - Paulo Sérgio Pinheiro

it never used and will never use toxic gases against its people because it does not possess them in the first place and it considers the use of such gases a moral crime that must be condemned'.

•Of great coincidence, Eye Spy notes the Israeli attack on the WMD factory took place on the exact 10th anniversary date of the Mossad-launched operation which resulted in the destruction of Syria's covert desert-sited nuclear reactor.



Syrian Scientific Studies and Research Centre

SSRC Scientific Studies Research Centre

Established around 1970, the Scientific Studies Researchers Centre (SSRC) or Centre D'Etudes et de Recherches Scientifiques (or CERS), at Masyaf, has overseen Syria's, nuclear, chemical weapons (toxic) and missile producing programmes. In 2005, US President George Bush, on guidance from the CIA, stopped American companies from trading, liaising or generally performing any interaction, including academic, with the SSRC. A decade earlier, the CIA had begun monitoring its activities, and noted many covert deals were being conducted and agreements signed. In 2010, the Mossad discovered shipments of weapons from the SSRC were being sent to proscribed terrorist groups in the Middle East. In 2013, Tel Aviv authorised attacks against sites linked to the SSRC.

In April 2017, following the chemical airstrike at Khan Shaykhun, Syria, the US again imposed sanctions against the SSRC and nearly 300 employees for its alleged role in the attack. The SSRC plant at Masyaf was completely destroyed by Israeli Air Force (IAF) warplanes in early September 2017.



IAF F-16



'Syria affirms that it never used and will never use toxic gases against its people...'

Syrian Ambassador to the UN Hussam Eddin Ala

ALL IS WELL RUSSIA'S HANDEL

Signal Captures Imagination of a Global Audience

The media has once again focussed on a 'mysterious Russian radio station buzzing since 1970'. With speculation on the facilities purpose ranging from the ridiculous to the sublime. Eye Spy's Communication Editor, Paul Beaumont, reveals what's really behind the signal and its primary purpose

Known as 'The Buzzer' UVB76, or more recently ZhUOZ, the site is thought to have started life at a secluded location near the Moscow district of Povarovo. Following changes (maintenance period) in 2010 the station was relocated close to St Petersburg. A sister site is claimed to exist at Naro-Fominsk.



For years the station has transmitted a monotonous buzz on the frequency of 4625kHz but has been heard on others; 3219, 3824 and 3842kHz; and after 8.10pm 4585, 4666, 4705, 4745 and 6995kHz to name but a few additional frequencies. Prior to mid-2010 it emitted a warble at the top of the hour which ceased after the off air period.

A great many claims have been made about the presence of this station and what it is ultimately used for. Like many unknown signals, this has generated features which often border the ridiculous and are little more than speculation: for example, the Buzzer is an automatic nuclear retaliation launch system - or 'dead man's handle/switch'. On one occasion when the signal once stopped for a maintenance period, some on social media posted expectations of a first strike from Russia and declared the world doomed!



**Professor
David
Stupples**

Others believe the signal is a communication link between Moscow Center (FSB) and its global



BY PAUL BEAUMONT

network of spies. However, there is no evidence whatsoever to support this theory.

Professor David Stupples from City University, London, was a little more pragmatic: "There's absolutely no information in the signal. Occasionally the signal was interrupted by a voice reading a message."

Other grounded SIGINT specialists are aware that high power radio transmitters need maintenance to ensure good, efficient service.

Prior to these periods, the Russian Buzzer emitted poor signals as well as unwanted harmonics. Its actual use is therefore somewhat more mundane and given the massive land area of Russia one can understand why radio is used for its purpose.

Britain's world renowned Imperial War Museum describes the once important HANDEL system

Unit 1A control box for HANDEL, the UK public nuclear attack warning system operated between 1962 and 1992. The unit was a blue plastic box with cream painted metal top fascia plate, incorporating two dials, two microphones, a red operation button and a red tag operation key. Fitted with a cream insulated power cable and multi-pin plug.

Historical Note: This device was intended to deliver warning of a nuclear attack on the United Kingdom by cutting in to the speaking clock network to contact WB1400 units at Carrier Control Points. Only three examples exist, one at the United Kingdom Warning and Monitoring Organisation (UKWMO) HQ at Oxford, one at reserve HQ near Preston, and one in reserve.

LINKS: www.iwm.org.uk/

IWM IMPERIAL WAR MUSEUMS



COURTESY: IMPERIAL WAR MUSEUM



Russian Tupolev Tu-95 strategic bomber. NATO reporting name Bear

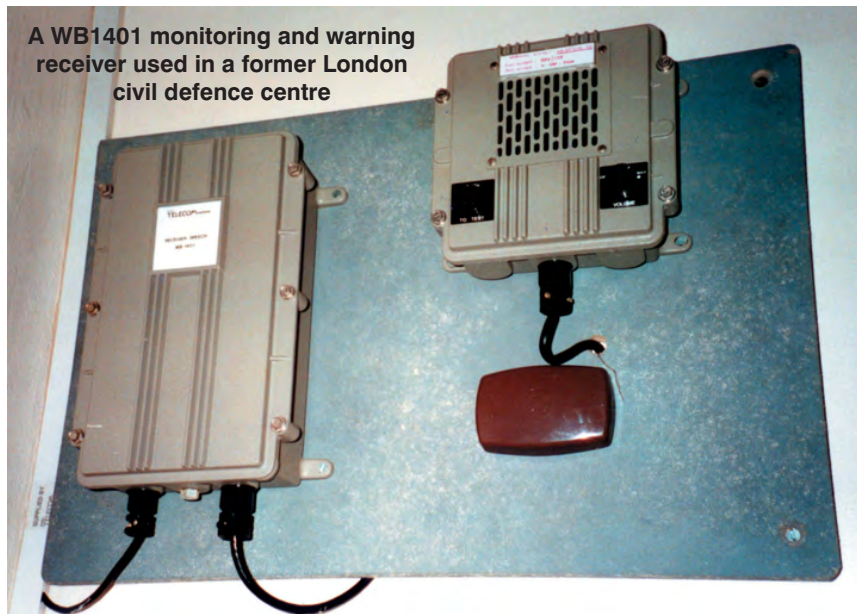
BRITAIN'S HANDEL

During the Cold War, Britain maintained an early warning system which relied in part on the telephone system. Signals were sent using the speaking clock [Dialled as TIM before the modern electronic system and 123 after privatisation]. A low frequency signal was sent to units operating in police stations and

probably other important locations notably by telephone lines. They emitted a 'seconds tick' which signalled an 'All's Well' message.

However, had nuclear war begun, the tick would have become a 'shrill warble' and certain recorded spoken messages heard. The only time this rationale changed was during a notified maintenance period. This equipment,

A WB1401 monitoring and warning receiver used in a former London civil defence centre



Listening to the 4625kHz signal

supplied via Britain's Home Office, was codenamed HANDEL.

CONCLUSION

To summarise, the 'mysterious Russian Buzzer' is simply Moscow's version of HANDEL; it will have other functions too, but as noted earlier, given the enormous land mass of Russia, radio is just one option used effectively to disseminate their 'All's Well' signal. The other known method is via telephone lines which are connected at a building in St Petersburg.

Radio or telephone, the signal is international, but nonetheless a simple 'All's Well' signal - but possibly with a military mobilisation content as yet not fully understood.



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

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

VOLUME 9



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



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



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



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



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



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



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



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

VOLUME 10



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



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



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



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



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



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



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



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

VOLUME 11



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



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



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



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



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



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



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



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

VOLUME 12



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



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



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



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



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



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



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



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

VOLUME 13



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



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



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



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



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



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



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



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

VOLUME 14



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



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



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



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

EYE SPY

INTELLIGENCE MAGAZINE

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 16 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!

SECRET HISTORY

LIFE



INSIDE THE LONDON CAGE REVEALED

BY DR HELEN FRY

A major new insight into one of the darkest secrets of British Intelligence...

THE VISIT

In June 1954, a team from New Scotland Yard's Special Branch drew up outside a flat at 19 Clarence Gate Gardens, the home of Colonel Alexander Paterson Scotland, nephew of famed Nobel Prize playwright George Bernard Shaw. At the same time, two other teams raided the London offices of literary agent John Farquharson Ltd and publishers Evan Brothers. Their brief from MI5 was the same - to seize all copies of a typed manuscript that ran to over 350 pages. Its author, Colonel Scotland, a retired officer of the Intelligence Corps, was about to go public with revelations as head of a secret wartime interrogation centre called the London Cage.

When the manuscript arrived back at MI5 headquarters and the Foreign Office, the introductory sentence to his second chapter caused alarm: *'Abandon hope all ye who enter here'*, he wrote.

It was in October 1940 that the War Office had requisitioned three adjoining mansion houses in Kensington Palace Gardens on behalf of the German Section of the Foreign Office, to open a clandestine interrogation unit known as the London Cage. Located in gated 'Millionaires' Row' and belonging to the Crown Estate, the street boasted one of the most exclusive and expensive residences in the capital and unlikeliest of locations to hold German prisoners-of-war. For the neighbours - the Russian Embassy tenanted next door and the



Colonel Alexander Scotland

wealthy magnates living in the other mansions - there was no inkling of what was going on behind the bravura Victorian façades of No.6-7, 8 and 8a Kensington Palace Gardens. Here the prisoners, who could not be broken under



A rare news cutting from the Evening News 1946 drawing reference to an incident at the London Cage

normal conditions of interrogation at any of the other eight 'cages' in Britain, were subjected to 'special intelligence treatment', designed to break their will to resist. As a transit camp, the London Cage should have appeared on the wartime lists of the Red Cross. It did not... because officially it did not exist. Its commanding officer Colonel Alexander Scotland, a tough maverick 70-year old military man, set the cage rules and this is where the controversy began.

In the prison quarters at 8 and 8a Kensington Palace Gardens, any trace of the former glory of the house had long since disappeared. Rooms on the first floor were transformed into cells with cold bare floors, a single bed, a chair and chamber pot. Life was run on strict discipline, enforced by guards from the Scottish and Irish Guard Division: they were both tough and effective. Sgt. Prion of the



8 and 8a Kensington Palace Gardens 1938. The photograph was taken by the German Section of Britain's Foreign Office as they sought premises for 'special purposes' in the event of war

Grenadier Guards could "cow these brutes (the SS) into complete obedience to cage rules." Close examination of declassified files now reveals that a very different picture emerges of the grim world in the basement where the five interrogation rooms were located. Out of bounds to most Cage personnel, it was here that contraventions of the Geneva Convention were alleged to have taken place. The interrogators had one primary objective: *'To assist MI6 and MI5 in gaining information by interrogating special suspects whose examination under military conditions offered to yield results'*. Soon,

mistreatment of uncooperative prisoners extended to a variety of methods usually associated with Soviet Russia: both physical and psychological, including the threat of 'Cell 14'.

Within six months of opening, the London Cage became embroiled in an internal heated controversy between MI5 and MI6 over the use of violence and unorthodox methods during interrogations. Colonel Scotland's early prisoners were U-boat crew and German air force personnel who potentially had valuable operational intelligence, but also details of new



Latchmere House - Camp 020



1942. Captured German soldiers



Lieutenant Colonel Robin Stephens

advanced German technological developments in weaponry and military equipment. The stakes were high. Britain needed the information which German prisoners held in their heads, knowledge which could affect the outcome of the war. Did the ends justify the means?

TRUTH DRUGS

Scotland already had a reputation as "a man of strong personality with a formidable reputation as an interrogator." He had made a scheduled visit to Camp 020, the covert MI5 interrogation of Latchmere House at Ham, near Richmond. Camp 020 housed captured German spies who were 'turned' to work as double agents for the British as part of the famous Double Cross System. It was there that Scotland struck a prisoner during interrogation. The MI5 Commandant, Lieutenant Colonel Stephens,

banned him from visiting the place again, but ironically Stephens too would face similar allegations at a site in post-war Germany (No.74 CSDIC at Bad Nenndorf). Revelations of physical abuse at the London Cage are controversial enough, but something far more sinister emerges - that Scotland was experimenting with 'truth drugs'. Already on the visit to Camp 020, he was caught wielding a syringe of truth serum, poised to inject a prisoner. Was he a maverick acting alone or with the sanction of the intelligence services? How did this tie in with the experimental use of truth drugs by Naval Intelligence and MI6 at this time?

For all the controversy that continues to surround methods of interrogation (brought again to the fore in recent times by US President Donald Trump - i.e. water-boarding), it is easy to forget that from 1945 until 1948, the London Cage became the War Crimes Investigation Unit and, according to those in the know, "the most important such centre outside Germany." Many high ranking Nazi war criminals and SS officers passed through its doors, having been hunted down by Scotland's own specialist teams roaming Europe to bring them out of hiding. Without Scotland's dedicated teams there would have been no justice in their cases. Amongst them were commandants from the liberated concentration camps, also SS General Sepp Dietrich, General Kurt Meyer, General Manstein, General von Falkenhorst, SS Colonel General Brochardt, Field Marshal Kesselring and Field Marshal von Rundstedt. One of the most loathed prisoners ever to cross the London Cage was SS General Fritz Knochen, responsible for the slaughter in cold blood of 124 surrendering British soldiers at Paradis in France in July 1940. He was described by Colonel Scotland as "a Nazi of the first order,



Another view of 8 and 8a Kensington Palace Gardens



Russian Embassy today -
6-7 Kensington Palace Gardens



Members of the SS unit
which carried out the Le
Paradis massacre



Colonel Scotland befriended Field Marshal Albert
Kesselring (centre) at the London Cage



Farmhouse where the
infamous Le Paradis
massacre took place

the worst order, a German who had dedicated himself to brutality; irresponsible in the possession of power, ruthless in execution." The London Cage also examined the major war crime committed at Stalag Luft III where 74 Allied airmen tunnelled out of the camp, known as 'The Great Escape' and immortalised in the famous film.

CONTRAVENING THE GENEVA CONVENTION

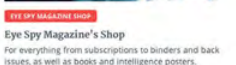
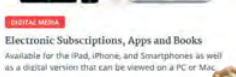
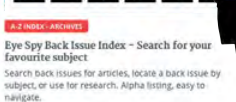
Claims of brutality, use of torture and psychological abuse surfaced again against the London Cage - this time very publicly during the war crimes trials - and Scotland faced serious charges that threatened to derail the Prosecution's case against the war criminals. The accusations extended to beatings, trampling on fingers, kicking, using a hippopotamus whip (a shambok), using an electric device to extract confes-

sions, and allegedly alluding to the fact that prisoners could "vanish without trace." When the International Red Cross sought entry in 1946, permission was firmly denied. Under oath in court, accusations of contravening the Geneva Convention were refuted by Colonel Scotland.

When the doors finally closed on 6-8 Kensington Palace Gardens in 1948, the intel services hoped that would be the end of the matter. But Scotland's unpublished memoir of 1954 offered a detailed account of life in the Cage that revealed unorthodox practices during the interrogation of German POWs. ➤

A shambok was used along with other devices to
extract information from German POWs





INTERNATIONAL EYE SPY INTELLIGENCE MAGAZINE

Visit the world's
most popular
independent
intelligence
website today

100%
SECURE
easy to
use shopping
cart!

INTELLIGENCE

24 Hours a Day

eyespyimag.com

20 MILLION HITS A MONTH!

JOIN US ALSO ON



www.facebook.com/EyeSpyMagazine



After impounding copies of the manuscript, MI5 consigned them to a basement at the War Office under 'lock and key'. Scotland himself was threatened with arrest under the Official Secrets Act if he published a single word. But the War Office knew it could not hold out for long. The memoirs could be published in America and the fall-out felt across the Atlantic. A deal was struck and Scotland published his book in 1957; it was heavily redacted by MI5. The intelligence services had everything to lose from revelations about methods used during interrogation. This was at a sensitive time in the Cold War when tensions were already heightened between East and West. What ended up on the cutting room floor was at least half of the manuscript, including all examples of methods of interrogation, anecdotal stories about specific prisoners, examples of conversations with prisoners, and life generally inside the cage. Scotland withheld any mention of truth drugs and certain methods of torture. When the official files were finally released into the National Archives in the 1990s, some were clearly missing and subsequently confirmed by the Ministry of Defence to be "contaminated by asbestos and destroyed by flood water."

Even today, there is a sensitivity in official circles about any mention of the London Cage, especially the four suicides whose names have never been released by the British Government or the Coroner's Office. Why the secrecy? But, in an era when democracy is threatened by global terrorism, perhaps it really isn't the time to open a public debate on appropriate methods of interrogation for our times.

ABOUT THE AUTHOR



Helen Fry has written over 20 books, mainly about the Second World War with a particular specialism on the 10,000 Germans who fought for Britain; as well as intelligence and espionage. In 2015, the *Guardian* nominated her book *Spymaster: The Secret Life of Kendrick* (Thistle Publishing: 2015) for the St Ermin's Hotel Intelligence Book Award. Helen has also published *The M Room: Secret Listeners who Bugged the Nazis* (Thistle: 2015). She has been interviewed on The One Show (BBC 1), Channel 4 documentary *Spying on Hitler's Army* (2013), ITV's *Britain's Secret Homes* (2013) with Sir David Jason; and Channel 5 for *The Hunt for Hitler's Missing Millions* (2014).

• Helen Fry's book *The London Cage: The Secret History of Britain's WWII Interrogation Centre* was published by Yale University Press in September 2017.

SPY CUBA

**US Diplomatic Staffers
Targeted by Unknown
EW Weaponry**

RUSSIAN INTEL GAMES?



CIA suspects new advanced Russian acoustic weaponry used against US diplomatic residences in Cuba

In late 2016, a number of US diplomatic staff and visiting family members working at the country's embassy in Havana, Cuba, began reporting hearing loss, nausea, headaches and balance disorders. Since then, the incidents have continued to occur on the island leading to some officials actually requesting their assignments be cut short. Others simply returned home.

US military analysts believe sophisticated devices producing a penetrating noise outside the audible range of humans, may well have been deployed to target staff residences. The latest reports surrounding the phenomena occurred in August 2017. In total, 20 people have been treated.

Washington has now threatened to close its embassy if attacks continue.



Former US Secretary of State John Kerry at the reopening of the US Embassy in 2015 - five decades after diplomatic relations ceased



"Victims of a health attack..."

US Secretary of State Rex Tillerson

Since February 2017, officials from various US Government agencies, including the FBI, have investigated who and what could be behind the incidents. State Department spokesperson Heather Nauert, said: "We can't rule out new cases as medical professionals continue to evaluate members of the embassy community." She described the situation as "unprecedented."



US Embassy,
Havana, Cuba



Eye Spy was informed, that despite various covert searches on the island and readings taken from measuring and detection machinery, no rogue sound emitting devices, generally referred to as sonic and ultrasonic weapons (USW) have been discovered. Some Americans are still affected. Nauert said the victims "suffer symptoms at different times, and they are different in various people. Let me just reassure you that this is a matter that

we take very seriously. It is a huge priority for us and we're trying to get them all the care that they need." Doctors who evaluated American (and Canadian) diplomats working in Cuba, diagnosed them with conditions akin to mild traumatic brain injury and damage to the central nervous system.

The Cuban Government has denied responsibility and said it had launched an "exhaustive, high priority urgent investigation." Privately, a number of officials told their US counterparts a "covert sonic device" may have been deployed by an intelligence service of a third country. The country referenced was Russia. US Secretary of State Rex Tillerson, confirmed the staffers had been "victims of a health attack."

Either way, the US State Department were none too happy, and in May 2017, two Cuban officials working at the Cuban Embassy in the United States were asked to depart. The

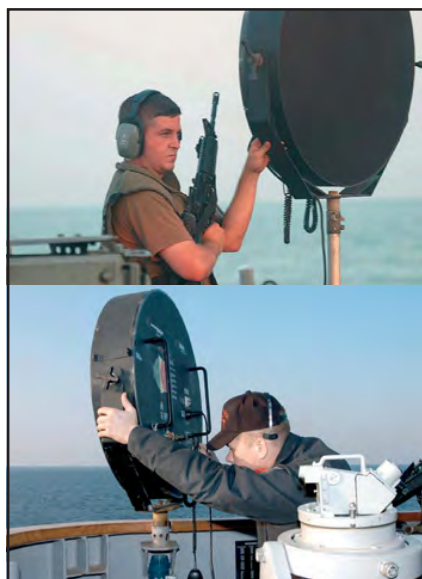


reason? "Failure to keep American diplomats safe... a breach of the Vienna Convention." Many analysts believe it was a direct response to what Washington believes was a deliberate attempt to sabotage its diplomatic mission in Havana. Full diplomatic relations, of course, were restored just two years ago after five decades of Cold War negativity and suspicion.

SONIC WEAPONS

Sonic and ultrasonic weapons (USW) operated by military and security forces of various types that use sound to injure, incapacitate, or kill an opponent are currently in limited use or in research and development stages. High-power sound waves can disrupt or destroy the eardrums of a target and cause severe pain or disorientation usually sufficient to incapacitate a person. Less powerful sound waves can cause humans to experience nausea or discomfort. The use of these frequencies to incapacitate has occurred both in counter-terrorist and crowd control settings.

Long-range military acoustic devices have been used deter pirates in seas around Somalia; police forces have used sound cannons against protesters, for example during the G20 summit in Pittsburgh and the Dakota Access Pipeline protest in South Dakota. The IDF (Israeli Defence Force) operate a device called 'The Scream' which results in dizziness and nausea. In the UK,



US Navy operated
Long Range Acoustic
Devices (LRAD)





Ground-based unified electronic warfare system on display at the MAKS-2015 International Aerospace Salon near Moscow



New York City Police operate a Long Range Acoustic Device (LRAD)



© VADIM SAVITSKI/SPUTNIK

Russian Defense Minister Sergei Shoigu and Cuban Minister of the Revolutionary Armed Forces, Corps General Leopoldo Cintra Frias visit the tank division of the Revolutionary Armed Forces of the Republic of Cuba

simple magnetic acoustic devices have been used to deter teenagers from loitering around shops. However, it is the more advanced machinery and technology, much of it still secret, which some officers in the FBI and CIA, believe may have been used against US diplomatic staff in Cuba.

EYES ON RUSSIA

In October 2016, Russia announced it had developed and successfully tested radio-

electronic weapons systems "unmatched anywhere in the world." A representative of Russia's United Instrument Manufacturing Company (OPK) - the lead company in charge of production, said the new technology falls under the somewhat loose term "weapons based on new physical principles." The grouping includes armaments that employ physical processes and phenomena not generally used in modern weapons. "Laser and sonic weapons are among other examples of such technology," said an OPK official.

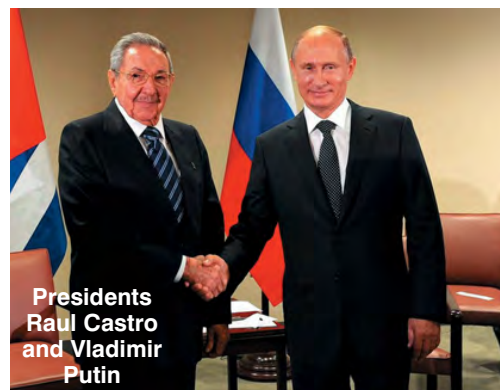


A US Navy security unit from the USS Anzio arrest members of a suspected pirate skiff in the Gulf of Aden



2015. President Obama with Cuban President Raul Castro

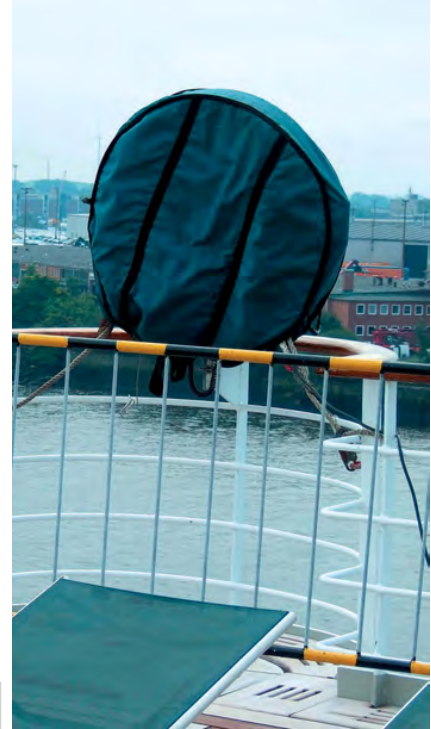
Naturally Russian officials did not disclose how, where and on 'what' the equipment was tested on. However, intelligence sources believe some field testing was performed in Serbia, and that a new type of Electronic Warfare (EW) weapon could have been used in Cuba. ➤



Presidents Raul Castro and Vladimir Putin



RMS Queen Mary. Right: A Long Range Acoustic Device (LRAD) fitted on the cruise liner as a counter-measure



"Return to Cold War tactics..."
Lt. General Kenneth E. Tovo

COLD WAR SUSPICION RETURNS

Russia operated the huge electronic intelligence (SIGINT) base in Lourdes, Cuba from 1967 until 2001. The spy station was the largest of all overseas Soviet intelligence centres with over 3,000 personnel, including a major KGB intelligence unit, military scientific arm and various armed forces facilities. After the Soviet Union collapsed, the base was run-down but a small Russian intelligence element remained. It was almost certainly responsible for blocking US radio broadcasts to Iran, and for the next decade, continued to support Moscow operations in North America - acting as a liaison facility to the country's navy and air forces.

Since 2014, there have been a number of authoritative reports that Russia is considering reopening its former spy base.

In Moscow earlier this year, retired KGB Lieutenant General Nikolai Leonov, a close

friend of President Vladimir Putin, voiced Russia's [continued] "considerable military interest in Cuba" during a presentation of his new book *Raul Castro: A Man of Revolution*. Leonov first met Raul Castro



NIKOLAI S. LEONOV

in the 1950s and again at the time of the Cuban Missile Crisis in 1962, when he received numerous intelligence reports from Cuban and Russian agents in nearby Florida. His experience and knowledge of intelligence happenings on the island is unsurpassed.

Today, Russia continues to have a presence in Cuba and despite former President Obama's effort to restore relations, there is much suspicion. The EW events have only conspired to lead many analysts to believe Russia "has never gone away." Indeed, Lt. General Kenneth E. Tovo of US Southern Command in testimony to Congress said that Russia's aim is the same as it was in the Cold War: "To erode

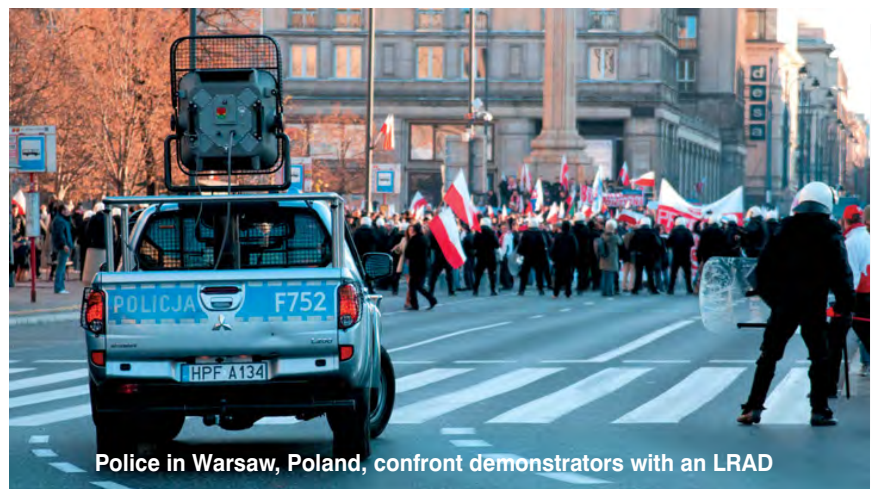


Satellite image showing the Lourdes spy site

US activities in the region. Russian influence is back in Latin America in a big way, along with a clear return to Cold War tactics."

President Trump has repeatedly criticised Raul Castro's authoritarian regime and Obama's renewal of diplomatic and economic relations with Cuba.

- One Canadian diplomat has also been treated for an acoustic injury whilst working on the island.



Police in Warsaw, Poland, confront demonstrators with an LRAD

The Deceptive Factor

IN THE INTELLIGENCE CYCLE



MIKE FINN looks at a number of simple ways in which our mental vulnerability works, how it can be exploited, and the intelligence research facilities that specialise in this kind of science; perhaps equally as important, the type of operations it can be applied to

INTELLIGENCE AND THE MIND

After the last article you may wonder about the vulnerability of the mind in the face of psychological operations in the intelligence cycle. Unlike a computer, the brain processor does not have a security programme to protect us against viruses, spam, trojans, and the like. There are various government organisations worldwide that engage in psychological operations and research. America's DARPA (Defense Advanced Research Projects Agency) is one such agency. This organisation has immense government resources available and specialises in all fields - enhancing both overt and covert military endeavours.

In the neuroscience area, one research direction is Transcranial Magnetic Stimulation (TMS), this uses electromagnetic induction on the brain to reconfigure certain thought processes. Another aspect involves a genetic code for NMDA (N-methyl-D-aspartate), thought to enhance learning and memory. Going for long periods without sleep could be a valuable military asset. The brain hormone

called 'orexin A' could fit that bill, not only does it restore wakefulness, but apparently obviates the grumpy side effect.

In Britain, work has been conducted for many years on the implant of microchips in the brain, in order to facilitate access to greater mental knowledge. This type of research comes from ingredient and component related methods of mind and brain manipulation; as ever, the stumbling block is biological rejection of non-biological material.

JTRIG - JOINT THREAT RESEARCH INTELLIGENCE GROUP

Neuroscience plays a vital role in understanding mind alteration through simple manipulation. The early study of conjuring helped the intelligence world open doors; neuroscience actually entered and explored the room. During the Nicaraguan conflict of the 1980s, the CIA produced a manual of psychological tactics, which was apparently aimed at manipulating opposition groups and highlights the mental interplay of those times. However, more



'hands-on' use of these skills are implemented by such organisations as JTRIG (Joint Threat Research Intelligence Group), mentioned in earlier articles. ➤



Edward Snowden appears at a cyber conference via a video link



GCHQ headquarters, Cheltenham - controllers of the JTRIG. The unit was exposed by the release of thousands of NSA documents by Edward Snowden showing its research and techniques. These papers showed they were distributed to members of the global Five Eyes 'syndicate'

In recent years the basic concepts of men such as Harry Houdini and Mulholland have been superseded by the advance of neuroscience. The intelligence world has concluded that cognitive systems are fragile and vulnerable; the doorway to this has been through the gradual developments I have described previously. There are various establishments around the world that are now peeking into the mind's vulnerability. One such organisation that has been highlighted in the public eye recently is the above mentioned JTRIG. It's objective (research) revolves around extremists, financial scams and various other political agendas.

JTRIG is reputed to have expertise in psychological and behavioural sciences, in particular, how human behaviour, perceptions, thought processes, as well as cultural and perceptive

parameters can be manipulated. These strategies rely on achieving their goals by exploiting the weaknesses of the mind and the vulnerability of misconception and conceptual reinforcement. As an element of GCHQ, JTRIG links to many other security and police organisations to achieve similar goals. However, PSYOPS (psychological operations) are worldwide, mind hacks are an easier way to discredit, diffuse and disperse what may be considered anti-social threats, both in daily life and through the Internet. World intelligence agencies are now exploring these areas.

Vulnerability begins with what is called the subjective mind, because we only 'perceive' the objective world (real world). This means that our cognitive knowledge, gained through the five senses, takes samples of the real world and relays this information to the brain,

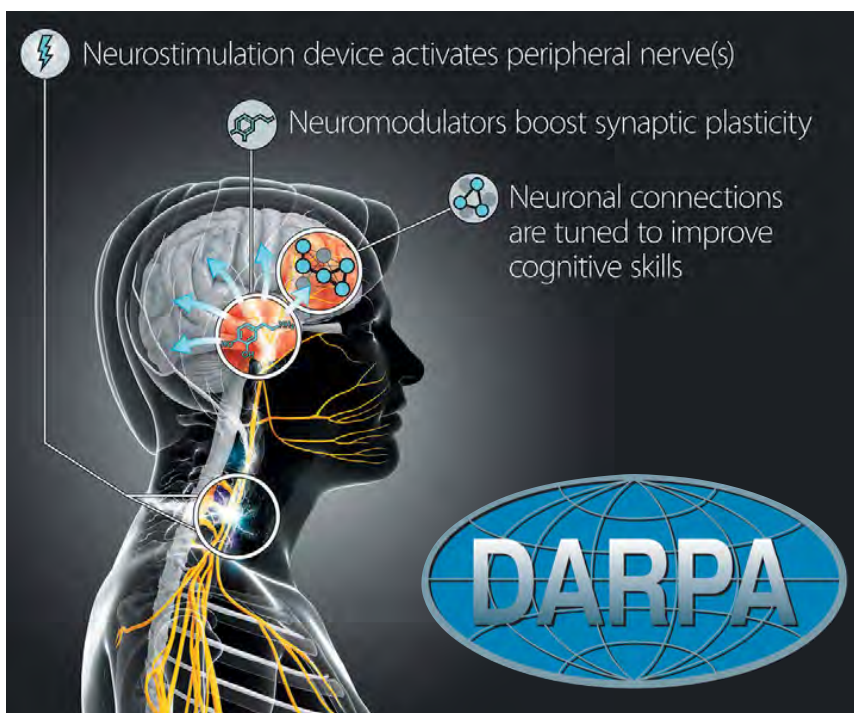
where it is processed to create a subjective image, based on the information received. However, this is clouded by the way our life conditioning causes us to interpret the information. In short, the real world and the mind's subjective impression of the world are not the same. It is in this area that the processes which create a subjective picture can be manipulated, in order to serve whatever purpose the controller wishes. Our perception of reality is both malleable and vulnerable.

MISINFORMATION AND PROPAGANDA

Humans are constantly bombarded by misinformation and propaganda, on both the domestic and intelligence front. Much is to do with the manipulation of our cognitive abilities.



Afghanistan, December 2001. A US Navy sailor hands out leaflets announcing a major bounty for information to the detention of Osama bin-Laden



DARPA: Defense Advanced Research Projects Agency

DARPA has long been engaged in important scientific work, much of it of relevant to the intelligence and military world, including that involving the mind and brain. One research project enabled earlier this year was the Targeted Neuroplasticity Training (TNT) programme. This is an effort to enlist the body's peripheral nervous system to achieve something that has long been considered the brain's domain alone: facilitation of learning. The crux of the wide-ranging programme is to identify optimal and safe neurostimulation methods for activating 'synaptic plasticity' - a natural process in the brain, pivotal to learning, that involves the strengthening or weakening of the junctions between two neurons - then build those methods into enhanced training regimens that accelerate the acquisition of cognitive skills.

TARGETING EMOTIONS BY COVERT MEANS

Edward Snowden's cache of stolen NSA files included a number of documents related to the work of the JTRIG and distributed to the 'Five Eyes' organisations. These papers include details of a variety of data which could be associated with PSYOPS (electronic) and mind manipulation under the banner of 'The Art of Deception: Training for On-line Covert Operations'.

Needless to say, the main thrust of the material was to inject material into various parts of the Internet (including media) to influence, disrupt and deceive. The papers provide an intelligence overview of how humans interact and perceive various information and news. And just as important, evidence if needed that the world of intelligence regards mind manipulation as a priority subject.



Gambits for Deception

SECRET//SI//REL TO USA, FVEY

Attention	Control attention Conspicuity & Expectancies	The big move covers the little move	The Target looks where you look	Attention drops at the perceived end	Repetition reduces vigilance
Perception	Mask/Mimic Eliminate - Blend Recreate - Imitate	Repackage/Invent Modify old cues Create new cues	Dazzle/Decoy Blur old cues Create alternate cues	Make the cue dynamic	Stimulate multiple sensors
Sensemaking	Exploit prior beliefs	Present story fragments	Repetition creates expectancies	Haversack Ruse (The Piece of Bad Luck)	Swap the real for the false, & vice versa
Affect	Create Cognitive Stress	Create Physiological Stress	Create Affective Stress (+/-)	Cialdini+2	Exploit shared affect
Behaviour	Simulate the action	Simulate the outcome	Time-shift perceived behaviour	Divorce behaviour from outcome	Channel behaviour

SECRET//SI//REL TO USA, FVEY



Let's take two simple domestic examples to illustrate the point. The first concept is that two similar products, one cheap and one expensive should never be put on display in close proximity: If they are apart, it has the same effect as the mind trying to remember two car registrations from different locations, at the same time. The pros and cons of the products blur, and a saccade comparison may see them as identical if they look the same on face value. The result will be in favour of the cheaper item as the illustration shows.

The second notion is more complex, it is about saving money on a product by minimising, but creating the illusion the product has remained the same: If a little is taken off a product that sells millions, the overall saving can be colossal. I only use the

chocolate bar as an example, there is no reflection on any reality involved. If a little changes over time, it usually goes unnoticed, a bit like watching a plant grow. If you look at the illustration (A). No one will notice if the content becomes smaller over time, as long as the packaging remains the same. (B).

By changing the design, some content can often be removed without notice. In fact a logo such as 'the new look gives you more', will create a better distracting illusion, without commitment to fact.

The third method can be encapsulated in the following: (C) By increasing the angle of the chocolate, some can be removed over time, without notice. (D). The depth of the recess can be increased overall. Provided the

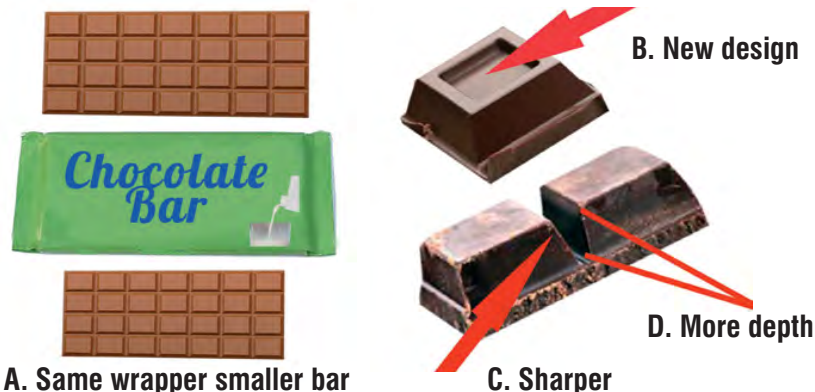
observable balance is kept, the status quo optical illusion remains.

I use these simplistic examples to show how cognition can be manipulated, how minds and choices can be changed, how things can only appear to be as they are, but have been subtly altered. In the commercial world such gamesmanship can just be a part of the industry strategy, but it sets a stage for mental fallacy, which opens another door. The intelligence world is seriously embracing this new science.

THE RAID AT ABBOTTABAD

Scientists are employed by some intelligence services who can conjure and manipulate a desired image, especially if it purports to be from a reliable source. If the truth escapes, then conspiracy theories can create a smoke screen. It's all part of the bigger picture. Take for example an event on 2 May 2011 - the

CHANGE WITHOUT PERCEPTION





US President Barack Obama and senior defence and intel figures at the White House following news that Osama bin-Laden had been killed. Pictured also is CIA Director Leon Penetta (left) and Admiral Mike Mullen

CIA-sponsored raid on Osama bin-Laden's compound in Abbottabad which led to his death. It was a massive political accolade for US President Barack Obama. The official public account relates how the CIA tracked down the terror chief's hiding place. Conversely, another version by journalist Seymour Hersh, suggested that Pakistan Intelligence (ISI) had Osama bin-Laden under house arrest at this venue, for at least five years prior to the raid. Official sources retaliated with severe criticism, rubbishing the comments. I am not



Research into the human mind, situational response and emotion is now considered extremely important by those working in intelligence and the defence industries. Undoubtedly some of the research conclusions are being used as a reactionary tool (manipulation and propaganda)

taking sides, just showing the importance of psychological manipulation of the political theatre.

The series began with Houdini, the intelligence world saw a gleam of light shine through a

crack in the door. Now the door is open and the room is being fully explored. In future articles we will continue to discover the developments and tangents of the deceptive factor and its use in intelligence.

LONDON'S GREAT ESCAPE

TUBE TRAIN IED FAILS TO EXPLODE

On 15 September, an explosion occurred at around 8.20am on a Tube train travelling on the busy Wimbledon to Edgware Road District Line. Fortunately, the device, concealed in what looked like a large paint bucket and placed in a shopping bag, only partially exploded. The blast was followed by a fireball that passed through the carriage injuring several people who suffered flash burns. Other passengers were injured as they fled the scene, some suffered crush injuries as



they made their way through a narrow exit at the Parsons Green Station. Security services arrived at the scene minutes later and the area was soon evacuated and cordoned-off.

Witnesses in the carriage reported a 'chemical smell', and some took photographs of the burning device that had wires attached - these looked similar to fairy lights. MI5 and New Scotland Yard (NSY) officers, along with specialists from the Defence Science and Technology Laboratory (DSTL), plus other forensic experts then engaged in a operation to secure all available evidence. At 10.00am, NSY declared the incident one of terrorism. Within hours, film footage secured from a number of the 12,000 CCTV cameras operational on the London Train network, had provided sufficient clues to identify at least one prime suspect. He was already known to both MI5 and NSY's Counter Terrorism Command (CTC). It seems this information was also passed quickly to CIA and FBI intelligence associates based in London who advised US President Trump.



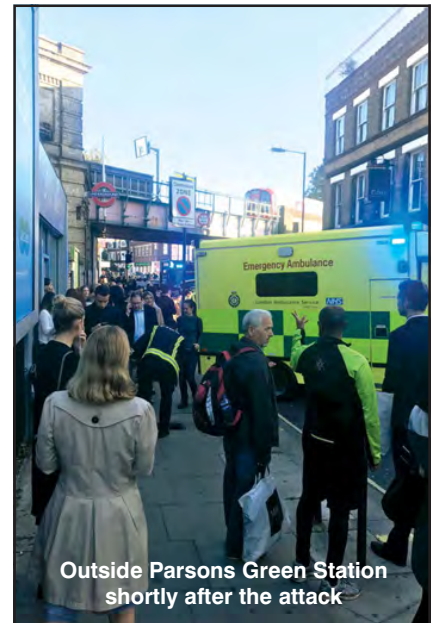
Parsons Green Station - scene of the explosion



A police roadblock near Parsons Green Station



The IED that failed to explode properly



Outside Parsons Green Station shortly after the attack

The President then made an error of judgement which could have alerted the bomber and associates by tweeting: *'Another attack in London by a loser terrorist. These are sick and demented people who were in the sights of Scotland Yard. Must be proactive! Loser terrorists must be dealt with in a much tougher manner. The internet is their main*

recruitment tool which we must cut off & use better! 'In the sights of...' relevant in this case.

Analysts recognised immediately the message was an indication MI5 knew his identity. This could have impacted on several hurried investigations and information-gathering operations that had been enabled. Prime Minister Theresa May was far from happy with the statement. "It's never helpful for anyone to speculate what's going on in an investigation," she said. A UK intelligence official also criticised the tweet, "an intelligence partner should not speculate." ➤



President Trump informed subject was known to security services



NSY Counter Terrorism Command (CTC) officers and police at the scene of the failed attack



Senior NSY Assistant Commissioner and counter-terrorism chief Mark Rowley confirms the incident was "one of terrorism"



Ten hours after the incident, and following various security meetings, Britain raised its threat level from Severe to Critical - meaning an attack is imminent. This was actioned because it was impossible to calculate if the

failed bomber and associates would attempt to strike again. Minister of State for Security Ben Wallace said: "This level was raised because there are very dangerous individuals on the loose." For its part, the terror group ISIS, via the Internet, soon began claiming responsibility for the attempted attack.

THE DEVICE

The unexploded bomb was removed by specialists and taken away by the DSTL for forensic examination. It is believed TATP explosive was attached to a timer allowing the terrorist time to simply exit the train. Officials are satisfied the IED was a crude, but nonetheless viable bomb. Eye Spy editors in London were told had the device exploded as intended, "it would have probably killed and injured many people."

Major General Chip Chapman, former head of the Ministry of Defence counter-terrorism element said: "This does not look like a high-

end explosive from ISIS such as TATP, or if it was, it failed significantly, the booster or detonator didn't go off." Indeed, had the device exploded properly, even the shockwave could have killed many people. Analysts have already likened the bomb to that built by the failed 7/7 copycat London bombers in 2005. Britain's most senior counter-terrorism officer Mark Rowley said: "We now assess this was a detonation of an improvised explosive device."



OPERATION TEMPERER

Hundreds of police (and MI5 officers) were assigned to the case, while ports and airports

Flash-burn injury suffered by Tube passenger Peter Crowley

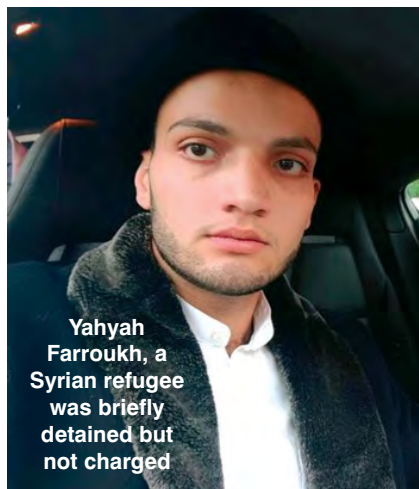


Enabling Operation Temperer - using troops to perform certain police and security roles, freed an estimated 1,000 New Scotland Yard officers, including specialist CTC units, to engage with the investigation and hunt for the terrorists





CCTV still showing alleged bomber carrying explosive device



Yahyah Farroukh, a Syrian refugee was briefly detained but not charged



Police carried out an extensive search of a house in Cavendish Road, London, reportedly connected to the alleged bomber



Minister of State for Security Ben Wallace

were alerted. NSY then advised that Operation Temperer (see Eye Spy 110) was activated allowing troops

to man certain police points; this freed additional police officers to be drafted into the search for the bomber.

SATURDAY - 16 SEPTEMBER

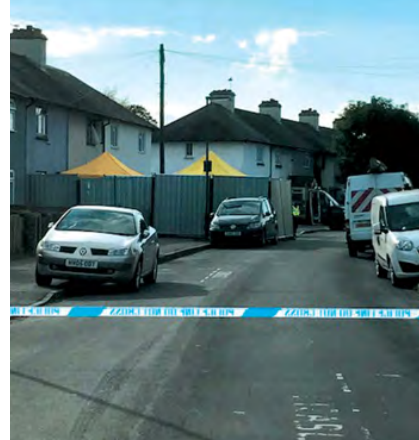
At lunchtime NSY announced that it had made a "significant arrest" in the departure area of the Port of Dover. Here an 18-year-old man, Ahmed Hassan, reportedly an Iraqi refugee, had tried to flee the country. Shortly after, armed CT officers raided a house in southwest

London and visited several locations. Sources said components described as a "bomb-building kit," had been recovered at an address in Sunbury-on-Thames - a 30 minute train journey from whence the IED used in the attack had begun its journey from Wimbledon. It later transpired the suspect once lived in the house, owned by a couple who had fostered over 200 youngsters and children and received an award for their work from the Queen. Shortly before midnight, a second suspect, Yahyah Farroukh, a 21-year-old Syrian refugee, was arrested in London.

Significantly, the UK threat level was then lowered.

TUESDAY - 19 SEPTEMBER

As MI5 widened its investigation, a 25-year-old man was detained by armed CTC and specialist Gwent Police and Welsh Extremism and Counter Terrorist Unit (WECTU) officers in Newport, Wales at 7.00pm. Ten hours later, and following a search of his address, two more men, aged 30 and 48, were also



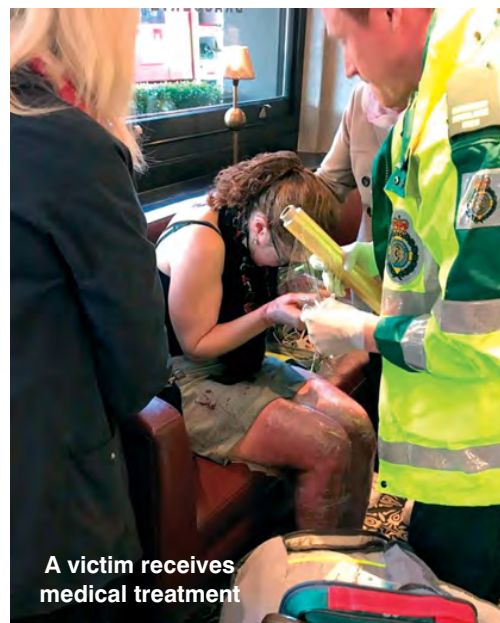
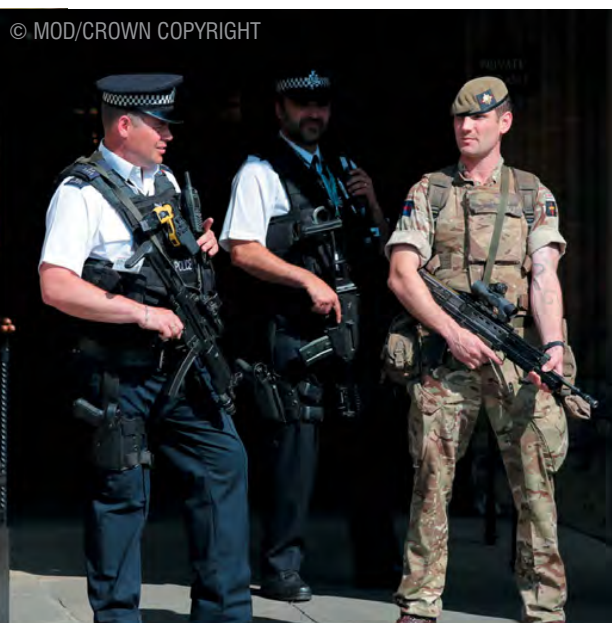
© SNAPPERJACK OF LONDON

arrested in Newport. On 21 September, Farroukh and the 48-year-old man were both released without charge after being questioned by senior MI5 and NSY investigators.

On 22 September, Ahmed Hassan was charged on suspicion of planting the IED on the train.



© MOD/CROWN COPYRIGHT



A victim receives medical treatment

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: \$35.00 EUROPE/WORLDWIDE £22.00

PRICE INCLUDES P & P AND ALL SHIPPING COSTS. OVERSEAS ORDERS ARE DESPATCHED AIR MAIL. PLEASE USE FORM ON PAGE 86
OR ORDER ON-LINE - www.eyespymag.com

**THE FIERCELY
GUARDED SECRETS**
of the
LONDON CAGE
will be revealed...

September 5th 2017

YaleBooks
www.yalebooks.co.uk



HB - £18.99

100 YEARS OF BRITISH SECRET SERVICE

Giant A1 Size. Each poster is produced on thick 170gm luxury paper and measures 841 x 594mm. Posters are sent air mail in hard tubes.

First released in 2009 to commemorate the historic 100th Year of MI5 and MI6 - these superb giant luxury posters are only available from Eye Spy

In Autumn 2009, MI5 and MI6 celebrated their 100th anniversary, the latter going operational just 72 hours before Vernon Kell, the head of the Home Section of the Secret Service Bureau sat down in his office. Kell began work on a Monday, while his counterpart, the eccentric first chief of the Foreign Section - Mansfield Cumming, decided to open his door on the Friday before. Even today, MI6 is proud of this fact, though it has been rumoured Cumming did this on purpose as both agencies should have started functioning at the same time!

These famous services have provided the basis for countless books, documentaries and even motion pictures. Eye Spy worked with a number of parties to create these posters; the photographs and text have been carefully researched and commissioned.

Besides providing an illuminating history of the journey of MI5 and MI6, the posters are packed with facts and anecdotes.

These superb posters capture the essence of both agencies and are absolutely unique.



PRICE INCLUDES SHIPPING AND PACKAGING!

MI5 Poster - Ref: MI5/100
UK £7.50 USA \$15.00 ROW £9.00

MI6 Poster - Ref: MI6/100
UK £7.50 USA \$15.00 ROW £9.00

MI5/MI6 Posters - Ref: Combo
UK £12.99 USA \$25.00 ROW £15.00

To secure your posters please use the form on page 86, or visit www.eyespyimg.com or telephone Eye Spy



'K'
Vernon Kell



EYE SPY BEST-SELLERS

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 86 or visit: www.eyespymag.com

EYE SPY INTELLIGENCE

COMPLETE

READ BY EVERY PRO

**VOLUME
2
COMPLETE**

Volume II
Ref: ESVOL2
UK £37.50
USA \$65.00
ROW £45.00



OUTSTANDING

**VOLUME
3
Issue 24 sold out**

Volume III
Ref: ESVOL3
UK £35.50
USA \$58.00
ROW £42.50



**VOLUME
4
COMPLETE**

Volume IV
Ref: ESVOL4
UK £37.50
USA \$65.00
ROW £45.00



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

E VOLUMES



IMARY INTEL SERVICE IN THE WORLD

VOLUME 6 COMPLETE

Volume VI
Ref: ESVOL6
UK £37.50
USA \$65.00
ROW £45.00



VOLUME 9 COMPLETE

Volume IX
Ref: ESVOL9
UK £37.50
USA \$65.00
ROW £45.00



COMPLETE YOUR EYE SPY COLLECTION

Volume Two numbers 9-16
Volume Three numbers 17-23
Volume Four numbers 25-32
Volume Five (see single issues)
Volume Six numbers 41-48
Volume Seven numbers 49-56
Volume Eight numbers 57-64
Volume Nine numbers 65-72
Volume Ten numbers 73-80
Volume Eleven numbers 81-88
Volume Twelve numbers 89-96
Volume Thirteen numbers 97-104



EACH VOLUME COMES WITH A FREE HIGH QUALITY EYE SPY BINDER



STANDING VALUE

VOLUME 7 COMPLETE

Volume VII
Ref: ESVOL7
UK £37.50
USA \$65.00
ROW £45.00



VOLUME 10 COMPLETE

Volume X
Ref: ESVOL10
UK £37.50
USA \$65.00
ROW £45.00



VOLUME 12 COMPLETE

Volume XII
Ref: ESVOL12
UK £37.50
USA \$65.00
ROW £45.00



VOLUME 8 COMPLETE

Volume VIII
Ref: ESVOL8
UK £37.50
USA \$65.00
ROW £45.00



VOLUME 11 COMPLETE

Volume XI
Ref: ESVOL11
UK £37.50
USA \$65.00
ROW £45.00



VOLUME 13 COMPLETE

Volume XIII
Ref: ESVOL13
UK £37.50
USA \$65.00
ROW £45.00



SECURE THE SECOND, THIRD, FOURTH, SIXTH, SEVENTH, EIGHTH, NINTH, TENTH, ELEVENTH AND TWELFTH YEARS' ENTIRE COLLECTION OF THE WORLD'S LEADING AND MOST POPULAR INTELLIGENCE MAGAZINE...



MAJOR RISE IN UK TERRORIST ARRESTS

The UK Government released data showing terrorism associated arrests reached record levels in a rolling 12-month period from 1 June 2016-2017. The Home Office statistics show a 68% increase.

New data shows 379 arrests, of which around 125 resulted in a charge; 50% of the suspects

were released. In the previous 12 months 226 arrests were made.

Neil Basu, Deputy Assistant Commissioner of the Metropolitan Police, said: "While the terrorist threat has increased in recent months, so has our activity; reflected by this significant increase in arrests. We're taking every possible opportunity to disrupt terrorist activity - be it making arrests for terrorism offences, intervening where there are signs of radicalisation, or working with communities to prevent terrorists operating in their area. Police, together with the security services, are determined to make the UK as hostile an environment for terrorists as possible."

MI5 and other security services are currently monitoring around 3,000 'high profile' targets perceived to be an imminent threat. Intelligence officials have also revealed between 20-30,000 others are on watch lists.

Around 200 people are still serving prison sentences for terrorism offences. Figures show 95% are linked to al-Qaida and ISIS since its formation six years ago.



**Neil Basu, NSY
Deputy Assistant
Commissioner**

LAST WORD

In August, New Scotland Yard announced that Firearms Command officers have been issued with body-worn video cameras (head-mounted) as part of an on-going initiative. Around 17,500 cameras thus far have been delivered to various overt security and patrol units in London



OFFICIAL EYE SPY ORDER FORM 2017

Ref	Price	Ref	Price

Total £ or \$

Name _____

Address _____

Post/Zip Code _____ Country _____

Method of payment [A] Cheque [] [B] Credit card []

Cheques payable only to: **'EYE SPY PUBLISHING LTD'**

Card number _____

Expiry date _____

Last 3-digits on reverse of card (security code) _____



UK, EUROPE AND REST OF WORLD

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



UNITED STATES OF AMERICA

Eye Spy Magazine, Empire State Building,
350 Fifth Ave, 59th Floor, New York,
NY 10118-0069, United States of America
Or Telephone TOLL FREE 877 309 9243



CANADA

Eye Spy Intelligence Magazine,
Canadian Bureau, Unit 102,
2054 Courtland Drive, Burlington, Ontario, L7R 1R8
Or Telephone TOLL FREE 877 309 9243

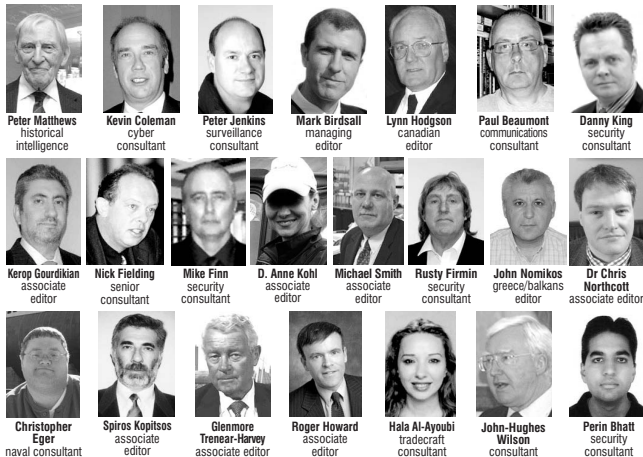
WE ACCEPT ORDERS VIA PAY PAL eyespy@eyespymag.com

INTERNATIONAL INTELLIGENCE MAGAZINE

UK editorial address and head office: Eye Spy Publishing Ltd,
P. O. Box 10, Skipton, Leeds City Region, BD23 5US, England
Telephone: 01756 770199 UK
Office hours: 12.00pm - 6.00pm Monday to Friday GMT UK

USA editorial address and head office: Eye Spy Magazine International,
Empire State Building, 350 Fifth Ave, 59th Floor, New York,
NY 10118-0069, United States of America
TOLL FREE: 877 309 9243 • SUBSCRIPTION & ORDER LINE ONLY
Office hours: 7.00am - 4.00pm EST Monday to Friday
E-mail: support@eyespyimag.com • Web Site: www.eyespyimag.com

senior editors, consultants and feature writers



EYE SPY INTELLIGENCE MAGAZINE AVAILABLE ON NEWSSTANDS IN 60 COUNTRIES



EYE SPY welcomes articles, photographs, case files, special reports, documents and newscippings on matters featured or associated with the type of material in this magazine. Text can be submitted in most formats or hand written. If you require your submission returned, please enclose a large self addressed and stamped envelope.

The opinions and views expressed by contributors do not necessarily reflect those of the publisher (ESPL) or editor.

EYE SPY SUBSCRIPTION RATES WORLDWIDE

Annual subscription rates include air mail posting and packaging (eight editions)

united kingdom	£29.95
united states of america	\$49.95
europa	£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 112



COMING SOON

THE NEW CT OPERATIVES

AVAILABLE LATE NOVEMBER 2017



Security is no accident... it has to be practised

Support Your Local Newsagent

The best way of ensuring that you receive your copy of EYE SPY is to support your local newsagent by placing a regular standing order. The newsagent will be able to deliver it to your door or reserve it in the shop for you to collect. If you have any difficulty, why not consider taking out a post-free annual subscription - see page 82



Dear Newsagent, please reserve or deliver a copy of EYE SPY on publication, starting with the next available issue

NameAddress.....

Post/Zip Code

Hand the coupon in to your newsagent, or a simple handwritten note is adequate

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 spylore. 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

**SPECIAL
NEW PRICE!
EXTENDED
2017**

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

