The Intelligence Trade

Most nations declassify some of their secrets each year but the unauthorised leakage of secrets to WikiLeaks has introduced a whole new ball game.

Security of classified information is always a problem, as a recently released government report disclosed that over 1000 Australian government laptops were stolen, lost or left behind in airport lounges and taxis in five years to 2003, and 537 of those were Defence Department laptops containing classified material.

Every year, new storage systems like iPads, tablets and mobile phones with Internet access add to the risk of loss of secret material. One can only hope that encryption systems are also improving.

Throughout this series, which will be broken up into groups of units, you will be encouraged to do some of your own research and references will be listed at the end of each session. In addition, research activities will be suggested at various points. Some subjects are so broad, for example, World War Two, that there are thousands of references on the Internet and countless books. I will name some references but in other cases leave you to explore further. Also, some of my knowledge has come from personal experience or has been obtained by extensive research at National Archives in capital cities and from the Australian War Memorial Archives in Canberra. What I have used is no longer classified but I hesitate to quote file numbers because some files are still listed as "*Not Available."*

Before I take you to the Garden of Eden some 6000 years ago, where the first signs of espionage emerged, I must lead you into what some call "The Shadow World," others call "The One-Way Mirror Room", and others liken it to "Alice In Wonderland".

Whatever you call it, nothing is what it seems

The intelligence trade is full of words that need some explanation.

1. AGENT-IN-PLACE or MOLE – an agent in a foreign country, often with access to commercial or government secrets.

2. AGENT PROVOCATEUR – a secret agent placed in a body of people to incite actions. The first one was in the Garden of Eden.

3. DEEP COVER AGENT - one who remains dormant, sometimes for years, until activated by a controller or handler.

4. DOUBLE AGENT - an agent of one country who is really an agent of another country.

5. LEGEND – a crafted history with false birth certificate and other documents prepared for agents-in-place or in deep cover. Less detailed legends, including false passports, are prepared for agents travelling to a foreign country for a short spell.

6. OWN ASSETS - citizens recruited by their country's intelligence body and used for specific tasks. Their names are never recorded as staff and they appear to lead normal lives in businesses that involve travelling. Their family will be unaware of carefully concealed assignments and this double life can lead to trouble.

Such assets usually enter a foreign country with their real identity and a valid reason for being there. They act in a normal manner and do nothing to draw attention to their real purpose. In some cases their valid passport may have been doctored or even duplicated to conceal visits to other countries – for example, it is best to have no Israeli visa stamps when visiting Muslim countries. For this and other reasons, an asset may have a second valid passport that is never kept at home, and in extreme cases this matches a legend.

7. FOREIGN ASSETS - nationals in a target country may act for personal reasons – revenge, dissatisfaction, etc – or are bought or blackmailed into providing services or information.

8. COVERT - concealed, secret, and hidden.

9. **OVERT -** open to view, obvious.

10. CONSPIRACY - an agreement to act in concert with others, sometimes with evil purpose.

11. TERRORISM - coercive and violent behavior undertaken to achieve or promote a particular political objective or cause, often involving the overthrow of established order.

Intelligence personnel often have their own in-house titles that are picked up by fiction writers and here are a few:

PLUMBERS are technicians who tap telephone connections, insert hidden microphones and TV cameras. They are part of a much larger signals interception body – Australia's Defence Signals Bureau (DSB), Britain's Codes and Ciphers Head Quarters (GCHQ), United States National Security Agency (NSA)

BURROWERS are research officers, experts in the analysis of documents, photographs and past files.

FOLLOWERS or TRACKERS are skilled in the surveillance of a "person of interest", either by foot or in transport.

I will explain other words that crop up as we travel.

At this point I should say that I am still old school, and often use "*Britain"* instead of "*United Kingdom."* It is one less word to type and most of her embassies still carry the words "*British Embassy"* on their facades.

Further, I always stress to my classes that I am neither a teacher nor a lecturer, just a teller of stories that are the result of much research, with some personal experiences that gave me the clues to know

where to find the buried files. Some of the events in my stories were hidden from government ministers at the time, and while many are now declassified, they are still hard to find unless you know where to look.

What used to be known as classified information in Britain is now called **Protectively Marked Information,** determined by the Cabinet Office and followed by all levels of government and the military, as well as any parts of the private sector that provides services to the public sector.

Five levels of classification are used, printed or stamped in capital letters in the centre of the top and bottom of each page of a classified document.

The highest Cold War classification was Umbra, a word that is defined as "*the part of a shadow from which the direct light is entirely cut off."* This happens during an eclipse, for example, where part of the shadow of earth or moon hides one of those bodies from the sun.

The word joined our language in the 16th century, and also denotes a "*phantom or ghost"* and came from the Latin that meant "*shade."* I'll talk later in the series about the joint UK/US "*VENONA"* project that broke thousands of Soviet messages during WW2 and the Cold War, to which some academic assigned "*Umbra"* as an appropriate security level.

UMBRA documents are kept under combination lock and never removed from the office unless transmitted in accordance with regulations. **ULTRA** is a slightly lower classification and documents so marked are highly restricted, even from ministers.

TOP SECRET classifies information released which could cause considerable loss of life, international diplomatic incidents, or severely impact ongoing intelligence operations. Prior to WW2, this was **MOST SECRET,** but it was renamed to conform to UK and US systems.

SECRET is down one level, and if leaked is still likely to cause damage to persons, public order or to diplomatic relations. This is the type of material that WikiLeaks was given and distributed.

CONFIDENTIAL is the next level down, and covers similar material to the previous two classes, but if such information was released it would not be so serious.

RESTRICTED is a lower level, and if released it could cause distress to individuals, adversely affecting the effectiveness of military operations, or to compromise law enforcement.

PROTECT is the lowest level of security, and used to restrict information that will cause some distress to individuals, cause financial loss or improper gain, prejudice the investigation or facilitate the commission of a crime or disadvantage government in commercial or policy negotiations with others.

NEED TO KNOW can be added to each of these classifications to separate groups of data for further protection.

LOCSEN is added to a classification if it has local sensitivity and may not be shown to local officials. **NATSEN** has national sensitivity.

EYES ONLY adds a further restriction to secret or above classifications. For example, **SECRET AUSTEO** = Secret Australian Eyes Only, meaning "this document contains code words and is only available to those specially authorised and listed as such".

The largest acronym is used by UKUSA Community (Five-Eyes) and is quite a mouthful – **AUSCANNZUKUSEO.**

The US military stores and communicates information about intelligence, operations orders and technical data on a classified Secret Internet Protocol Router Network (SIPRNET) and had a caveat NOFORN meaning no foreigners were allowed access. This restriction included the British and Australian troops fighting alongside the Americans in Iraq and Afghanistan. At times it went beyond the absurd.

British pilots and ground engineers using American F-117s and F-15Es weren't allowed to read parts of the classified pilot and maintenance manuals because they were marked NOFORN. UK Prime Minister Blair and Australian Prime Minister John Howard complained directly to the US President several times and In July 2004, Bush finally signed a directive, supported by Rumsfeld and John McLaughlin as acting director of Central Intelligence, that said NOFORN would no longer apply to the British and Australians when they were planning for combat operations, training with the Americans or engaged in counter-terrorism activities.

Frank Miller, chairman of the Executive Steering Group for Iraq, soon discovered that instead of giving the Brits and Aussies total access, the Pentagon had created a new, separate SIPRNET for them, rather than allow its allies access to the main SIPRNET that had years of information stored on it and which it did not want the British and Australians to see it.

Germany surrendered in WW2 on 7 May 1945, and on 2 September 1945, the official surrender of Japan was signed on the USS Missouri. September 2012 will be the 67th anniversary of the end of the Pacific War, yet some secrets about WW2 in all areas are still classified.

The Official Secrets Act is used in the United Kingdom (1889), Hong Kong, India, Ireland, India and Malaysia as a short title for legislation that protects state secrets and official information, mainly related to national security.

Australia uses *Part VII of the Crimes Act 1914 (Commonwealth), Official Secrets and Unlawful Soundings,* and one Crimes Act document I signed in 1945 is valid until "*death do us part",* as it refers to some of the algorithms and procedures used to break ciphers, binary codes and to interviews in 1958 with Eva Allyson (Evdokia Petrov) on Russian ciphers.

The United States does not have a broad-reaching Official Secrets Act, although the Espionage Act of 1917 has similar components. Much of that Act remains in force, although the Supreme Court has struck down some parts as unconstitutional because of the First Amendment.

Activity 1.1

Search the Internet for details of secrecylaws of other countries, for example, Soviet Union/Russian State, France, Germany, Japan.

Post your findings to the Course Discussion Forum

I began to gain my knowledge of military intelligence, codes and ciphers from an early age. My father came with his parents and siblings to Australia from England in 1913 and was a 21-year-old bank clerk when he joined the First AIF in Echuca, Victoria. He was as sergeant in charge of a Vickers heavy machine gun unit in France during some nasty battles including Vimy Ridge and Passchendaele during 1916 and 1917. He returned to Australia in 1920 after three years in England applying his business experience to the return of personnel to Australia and then sorting out some of the classified material for transfer to archives.

The bank kept their enlisted staff "*on leave while in service"* and transferred him to Queensland staff when he returned to Australia in 1920. He met and married my English mother after she migrated to Brisbane in 1921 with her widowed mother.

Here I digress, as I am wont to do from time to time, but never fear; like MacArthur, I shall return, but with less fanfare.

Here is a story that began in 1907, **during the Boer War.**

British cavalry officer Captain Edward Baker was wounded and finally rescued, but while he lay on the ground he fantasised about nurses on horses, riding through the battlefield to rescue him. After the war he pursued his fantasy and created an all-women volunteer group that would do just that, although later the ladies swapped horses for motor ambulances.

The group was titled *First Aid Nursing Yeo*manry and it wasn't long before the ladies, not the men, came up with an acronym for that - ***FANY***.

Activity 1.2

Follow the full story of these ladies in two World Wars at http://www.historylearningsite.co.uk/the-roll-of-british-women-in the-twentieth-century/first-aid-nursing-yeomanry/ (Early history and WW1),

https://en.wikipedia.org/wiki/First_Aid_Nursing_Yeomanry, and

*https://**en.wikipedia.org**/wiki/**William_Reginald_Hall***

The ladies served with distinction in France and Belgium during The Great War, later renamed WW1 because Hitler wanted to start another one. They were chosen carefully, for as well as the arduous and dangerous task of reaching the wounded, they also had to learn other skills – vehicle repairs, map reading, and communications with flags, blinker lights and wireless.

Admiral Sir Reginald Hall (see References**) –** nicknamed "*Blinke*r," due to a regular twitch of his eyes – was head of British Naval Intelligence in 1914, first as a captain, later rising to be an admiral and knighted.

Code breakers came under his command and he recognised the need to intercept and break German wireless messages. Interception stations were erected along the Channel coast and a team of rather unmilitary personnel – men and women who were linguists, classical scholars, crossword puzzle fanatics and lateral thinkers – were collected to break open the intercepted coded material.

Volunteers from the Naval College – Alistair Denniston and Dillwyn (nicknamed "Dilly") Knox – led the team based in Room 40 at the British Admiralty building, but as the workload increased they took over other rooms, and Knox took over Room 53 and installed a bathtub and chip-water heater where he seemed to do his best thinking.

Admiral Hall then started poaching selected members of First Aid Nursing Yeomanry, especially those who had been expert typists and shorthand writers before they joined as FANYS and who, when tested, showed above average skills in solving crossword puzzles of all types.

My Yorkshire mother was relieved from driving ambulances and joined the decrypting team. Yes, finally back to my mother.

She told me she had to take a puzzling code message to Dilly Knox in Room 53, and was always very careful to knock loudly and say "I*t is Eleanore, with a message. Are you decent".* He would often stay in the bath, with a towel discreetly draped, ponder while she held the paper in front of his eyes and then tell her what to do to break the message.

Many years later, when I was six, she gave me my first lesson in cryptography.

Twice a year we travelled to Brisbane from our country town and stayed with friends for several days. Mother loved to shop, but in the Depression she had to watch the pence and she showed me how she looked at both sides of price tickets**,** pointing to the letters on the back of the ticket that indicated what the store had paid for the item, while on the front, in pounds, shillings and pence, was the selling price. You can still find such tickets in antique and gift shops in tourist areas and small towns.

Ticket codes use different letters for the numbers from 0 to 9, and one letter for an oblique stroke or a dot. You could use A through to J for 0 to 9, and K for an oblique stroke, but that would be too easy for someone to break, so most stores used a word or phrase that did not repeat a letter and the staff could remember. Senior sales staff became adept at sight-reading the codes but a codebook was used at pricing and stocktaking times for all staff. Mother deduced her favourite clothing store's code word as FROCKSINVAL, a logical code word as this store was a frock shop in Fortitude Valley, Brisbane.

Finding a "crib" – a code breaker's term for clues to break the code – is the first step, and then you work backwards. In this example, the first ticket she read showed the retail price of 17/11 (shillings and pence). The letters FALV were on the back of the ticket and with only four letters, Mother assumed the cost price would be less than the selling price and one letter must be an oblique stroke.

Cost price - option one - 1, ?, /, ?; option two - ?, oblique stroke, ?, ?.

In option two, the first number cannot be 0, so is between 9 and 1. A cost price of 9/??, means a mark-up of nearly 80%, a bit steep in Depression years, and any lower cost price means an even greater rip-off. She discards option two and proceeds with option one, starting with a cost price from 10/?.

Already she has F=1 and in the third position, L=/. That leaves A and V, as either 0 or a range from 2 through to 9.

Decoding is a bit like a crossword puzzle, where a few letters let the rest fall into place, and after reading a few more price tags she has the complete code - F1 R2 O3 C4 K5 S6 I7 N8 V9 A0 and L= an oblique stroke or a dot, and she has found the store's code word is FROCKSINVAL.

After calculating the mark-up she would find the floor manager, flutter her eyelashes and begin to bargain, using a mind that ran like a mini-computer.

Small business owners did not change their codes very often, as the average shopper was not likely to be a code-breaker. Even larger companies, banks and governments hesitated before changing a codebook that might contain thousands of words or phrases.

Activity 1.3

Using some of my mother's ticket codes try to work out the cost to the retailer.

Two clues U=1 and D=/ to use in solving the cipher

You have three items -

Coloured crepe frocks sale price 7/11 Coded ticket for cost EDUU

Crepe nightdress sale price 4/11 Coded ticket for cost HDE

Boy's suit sale price 19/6 Coded ticket for cost UHDUI

Post your solution to the Course Discussion Forum

Depending on its size, it takes a while to create and distribute a new codebook, and the one used by the Bank of New South Wales (now Westpac) where I worked for three years before joining the AIF in 1943, had been issued in 1925, and was amended annually.

Japan faced a major problem with their codebooks during the Pacific War, with bases all around the Pacific and in Asia, and ships at sea. They were forced to send similar messages to different addresses, some in the old code and some in the new, until a revised codebook could be circulated. This was a bonus for our code breakers, who were familiar with the old codes and used a message in the old code to provide cribs to break the same message in the new code.

After working on signals and coding and ciphers in the Army from 1943 to 1947, I was discharged in Melbourne and married, a lass I'd met while training signallers at Balcombe who were heading for the Occupation Force in Japan. Later I gained a couple of degrees in accounting and costing and eventually became a business and computer consultant but the government never lost track of me and recalled me part-time for cipher consulting services from 1950 until 1975.

When I retired, my association with "*things secret"* gave me time me to delve deeper into what lay behind the secrets. Knowing what files to search for, I visited Canberra's Australian War Memorial and the National Archives of Australia and searched archives of other nations.

I have been asked from time to time "why don't you use all your talks as the basis for a book?" There are two reasons.

Many of my stories come from material that has already been published, and I acknowledge that in your references; also,

I would have to obtain clearance for any personal experiences, and this can be very difficult.

Here are some examples and also see References at end of this Unit.

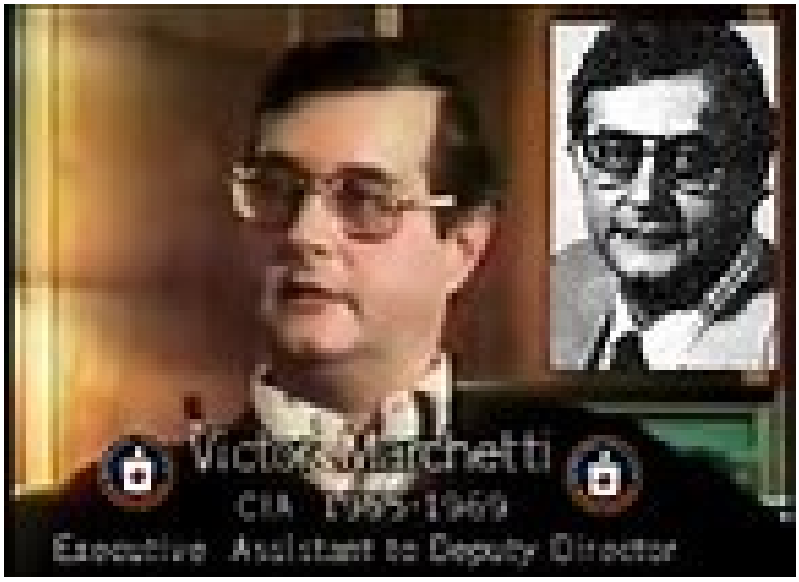

Fig 1.1 Victor Marchettti

American Victor Marchetti returned to university after serving in WW2 and majored in Russian Studies. He joinedCIA in 1955 and was executive assistant to CIA Director and the top analyst on Soviet matters when he retired in 1969. He and John D. Marks from US State Department Intelligence and Research department met in April 1972 and wrote a book entitled *The CIA and the Cult of Intelligence*.

Marchetti used "The" in front of "CIA", but most CIA personnel still follow a practice that goes back to its formation after WW2, when many of its officers were drawn from the wartime OSS and had graduated from upper class US universities such as Yale and Harvard. The insisted "*you don't use 'the' in front of God and you should not use it in front of CIA!"*

Under his retirement agreement, Marchetti was ordered to submit his manuscript for review, prior to any submission to a publisher. He did that in August 1973 and CIA immediately filed an injunction against publication and a judge ordered CIA to complete their review within thirty days. CIA lawyers returned to court with **339 portions** to be deleted. Some were only words but others were pages, so a trial was ordered.

In March 1974, two years after the book was started, the court decided many of the 339 portions did not seem to affect security, so, CIA reduced their claims to **168 passages, claiming "national security."** Judge Byrne decided only **27** sections could be deleted, then stunned CIA lawyers even further by ruling that the book be published with **bold type indicating the number of lines deleted, and where, and also ordered that the other 141 passages he had allowed be printed in bold type.**

The book was published in 1974 and anyone involved in intelligence was able to make a reasonable deduction as to the deleted items. It was of great interest to intelligence analysts of other countries, especially the Soviets, and a necessary item for researching intelligence and covert activities, as my copy is well worn.

Fig 1.2 Peter Wright

PETER WRIGHT combined with Paul Greengrass to write *SPY CATCHER – The Candid Autobiography of a Senior Intelligence Officer* – when Wright retired from Britain's MI5 in 1976, after twenty years' service that included the time of the Cambridge spies, Kim Philby and others (Burgess, Mclean, Blunt, Cairncross.)

Wright's book suggested that Roger Hollis, one-time Director General of MI5, was also a Soviet mole.

Margaret Thatcher's Government banned publication in 1985 and English newspapers could not publish any comments or reviews. However, the book was available legally in Scotland, as well as overseas, so its contents became well known.

Britain attempted to stop Australian publication, but lawyer Malcolm Turnbull – now a Liberal politician and Prime Minister – won the case for Wright in 1987 and a subsequent British appeal in 1988. Wright was barred from receiving royalties from sales in England, but sales elsewhere made him a millionaire. He died in 1995.

In 1965, a committee codenamed "*FLUENCY"* examined Hollis' service record in great detail, and unanimously concluded that he was the most likely source of leaks to KGB, but no action was taken as Hollis had retired from MI5 by then. A further review in the late 1970s was unable to decisively ascertain whether or not Hollis was a Soviet spy, and Prime Minister Margaret Thatcher grudgingly announced the result of that review in 1983.

Well, now you know some of the problems relating to research and publication of secret matters.

The Cold War ended a long time ago and Russian government has changed from dictatorship to a government that considers itself as democratic, but with a President who is an ex KGB officer and exercises control of Russia. Their intelligence agencies have changed names but still operate in the same way. A batch of Russian undercover agents in United States were arrested by FBI in 2010, charged and then exchanged for a few people the US wanted back from Russia. So the "*game"*" goes on, but one of the agents captured a lot of media attention because she fitted the image of a "*female spy."*

Fig. 1.3 Anna Chapman

Anna Chapman was born Anna Vasil'yevna Kushchyenko around 1982, when her father was a Soviet embassy official in Nairobi, Kenya, probably as an undisclosed KGB officer. Age 20, she earned a master's degree in economics with first class honours from Moscow University and moved to London in 2003, working for Barclays Bank and a few other companies for brief periods. She met Alex Chapman at a London Docklands rave party and they married soon after, meaning she gained dual Russian-British citizenship and obtained a British passport. Alex remained in London when she went to New York in 2007 as CEO of Property Finder LLC, a company selling real estate internationally on the Internet.

It ran at a loss for the first couple of years, and in 2009 it suddenly posted a profit and disclosed it had 50 employees. This interested FBI and an undercover FBI agent offered her a fake passport as a trap, instructing her to forward it to another spy. She was suspicious and made a series of phone calls to her father in Moscow who told her to hand the passport in at a local police station.

FBI had other evidence and arrested her shortly after and formally charged her in 2010. She was one of only two of the Russian agents who did not use an assumed name, and she and nine other detainees became part of a spy swap deal between the US and Russia, the biggest of its kind since 1986. They returned to Russia via a chartered aircraft in July 2010 and the British Home Office revoked her citizenship, upsetting her plans to return to the UK.

Before long, she was well known with cover photos on magazines, and also included on a list of Russia's 100 sexiest women. By January 2011, she was hosting a weekly TV show in Russia called *Secrets of the World;* in April 2011 she was modelling for Moscow Fashion Week and in June 2011 she became editor of Venture Business News magazine and was writing a column for Komsomolskaya Pravda. In November 2011, she gave a master class on business success at an IT conference for entrepreneurs who had paid £40 to attend the event.

Most "blown" agents are not as fortunate as Anna Chapman.

From 1 January 2012 Australian Cabinet records for 1982 and 1983 became available for the first time and annual releases make interesting reading. Some may be withheld for 50 years or even longer if deemed necessary, and even then many pages have redacted sections; matters deemed "*security problems"* are blocked from publication by Government orders.

In April 1959, Britain issued a "D" notice to stop any reference to British ballerina Margot Fonteyn and her husband being involved in an unsuccessful attempt to overthrow the Government of Panama. Files were not opened until 2009.

I have spent hours searching archives and not always successfully.

Internet access now makes research a little easier as national archives of many countries provide listings of most files held, and indicate their availability and whether digital copies can be downloaded. This where the fun starts.

Australian archival documents fall into three groups – OPEN FOR INSPECTION, NOT YET EXAMINED, and CLOSED.

Now you would expect files marked "*Open for Inspection"* to answer all your questions, but you can be mistaken.

In 1993 I asked Melbourne Archives for an "*OPEN*"' file titled "*Signal Intelligence 1945-1946."*

I didn't expect any problems after nearly fifty years, and a copy was produced within a few minutes, but when I began to flick through the thirty pages I understood why the lady who'd handed it to me had a wry smile. Many sections of the copy had been redacted (blacked out) and the Freedom of Information Act does not always provide answers.

The Archival Act can overrule FOI to protect personal privacy, or to protect the defence, security or international relations of the Commonwealth. I know of one case where files have deleted details of a young Chinese who aided a Z Special Unit operation in Java in 1943. He is now a retired businessman living in Indonesia.

"NOT YET EXAMINED"" files means no person with a sufficiently high security clearance has had time to peruse the file and decide if it can be opened to the public. Limited staff means it is not unusual to find 1940s files "*not yet examined."* You can request an examination, but don't hold your breath. However, if you can produce the required security clearance you may be allowed to see the file in a secure area, make notes but not take copies.

"*CLOSED"* files require an application, and you may even be subjected to an ASIO check that could take some months. If the file is then opened, there can still be many sections blacked out or pages withheld.

Unofficially, there is another group – "*NOT AVAILABLE",* meaning that for some reason or another, no one can find it.

You may draw your own conclusions from this story. **In 2004** I was researching the effect of chemical warfare on our Vietnam troops, Agent Orange in particular. A computer search of National Archives database listed "***File No. 886-R1-11, 'OPERATION DESERT',"*** with a brief description: "*re toxic chemical testing, sprayed around Gregory Falls, Innisfail, during 1964-66, prior to use in Vietnam."*

It was marked "*NOT AVAILABLE",* so I made a note to do a later search to see if it had been found. When I tried again the file number was still there, but the name and detail had vanished, and it was now marked as *"MISSING."* **A few weeks later the file number had been deleted.**

Months later I did a general search for "*OPERATION DESERT"* and it now had a different file number and referred to *"land clearing in West Australia."*

End of story!

I mentioned CODES and CIPHERS earlier and these two words have specific meanings but common-day usage has blurred the boundaries.

CODE is a type of language and **Morse code** is a type of code, rarely used these days as technology has found smarter ways to send messages.

Fig. 1.4 Samuel Morse

Samuel Morse (1791-1872) created the system and he and the Code are well covered on Wikipedia.

Morse used short and long bursts of audio sound known as dots and dashes – a dash is three times the length of time of a dot – to represent letters, numbers and various symbols that are assembled to compose a message.

A Morse message can be prepared for transmission in plain language and understood by anyone able to read Morse code, but it is more secure to convert the plain language into a secret form, either by a using an alphabetic or numeric code or a cipher, and then transmitting it in Morse code or some other means.

The recipient, or anyone intercepting such a message, must have a copy of the code or cipher, or have a means of breaking/cracking the message. Governments and businesses created code words for letters, words, phrases, numbers and symbols, to prevent enemies or competitors from understanding their cables or wireless messages, and compiled them into books, hence the name "code book", and distributed copies to users in various parts of the world, or within a country.

In my banking days, each Australian bank had its own codebook, comprising groups of several letters that represented a word or phrase. For example, "*Brisbane'"* was *KLZSA, "bank officer"* was YRPHY, and GSBKU meant "i*s transferred to."*

Each officer had a five-letter code name, so the Post Office handling a message transferring staff had no idea who was going where or when, but the bank manager soon knew who was being transferred when such a coded message was delivered.

Allied military assigned a variety of code names to major cities and towns during World War Two; BRISBANE was identified by BRAVE, 26752 and CHILLY at various times.

Codebooks have a problem, as code words in regular use become identifiable over time. These "crib", as they are called, allowed us to break many intercepted Japanese wireless messages, and their code words for cloud, rain, clear etc. meant we could often use our own met charts or messages from coast watchers to pinpoint their reporting stations. It also meant we could use Japanese forecasts to provide Allied pilots with confirmation of target weather. Two examples – MI KA KUMORI = cloudy and KA TU NE 10 = indicated the density of cloud. In those days we referred to cloud covering the whole sky as ten/tenths, but nowadays it is "eight oct", from the Greek, meaning eight. This is just a fancy way of saying eight/eighths – total cloud – but if only a small part of the sky has cloud it is one octa.

Governments and businesses use computers to create and maintain a database of unique names, often for a specific operation, but one needs to be careful to ensure it has no conflicting meaning.

In early 2010, NSW Police, ASIO and Federal Police were issued with a codename to cover the overall planning for President Obama's planned visit to Australia, later cancelled. The code name was BLUE GUM, innocuous enough as it referred to one of our native trees. When the US Embassy in Canberra received the code name they told our planners that it was a slang word in US for lazy African-Americans who refused to work, so it was changed immediately. A lot of paperwork had to be recalled and a new code name – still classified – was issued.

I doubt they had any problem in 2011.

CIPHER is another means of converting plain language into a concealed message and is quite different from CODE WORDS. Plain text is scrambled manually or by machine so as to make it unintelligible.

Hopefully, the recipient of the message is the only one with the means to decipher the message. For example, "*landing tomorrow"* might be scrambled as "*kgkab psdft jstwal."*

Depending on the sophistication of the cipher, it can be almost impossible for a cryptanalyst to provide a solution.

In later units I will explain how codes and ciphers are created and show pictures of some methods. The originals used script of the time – Latin, Roman, Greek, Italian French, Middle English and a variety of other languages but for simplicity my examples will all be in English.

Dates of events as recorded in old books and archives can be confusing because the calendars of some countries have changed over the years. The Japanese calendar was quite different to ours till the end of WW2, and I'll explain why when we reach the Pacific War (December 1941).

Britain continued to use the **Julian calendar** until 1752 before finally adopting the **Gregorian calendar** , a "*foreign calenda*r" created in 1582 to commemorate Pope Gregory XIII.

To add a little more confusion, historians are slowly changing BC to BCE – Before Common Era, and AD to CE – Common Era, to avoid upsetting other religions.

The idea is not new; in 1716, English Bishop John Prideaux used the word "*vulgar",* which comes from the Latin *word "vulg?ris" = "of or belonging to the common people",* when he wrote: "*The vulgar era, by which we now compute the years from the incarnation of Jesus."*

In 1908 the Catholic Encyclopaedia used the sentence: "***Foremost among these dating eras is that which is now adopted by all civilized peoples, and known as the Christian, Vulgar or Common Era."***

I am going to have two bob each way, using BCE where needed, but otherwise avoiding AD or CE.

References at the end of this unit include a link to a website with many supporting references and suggested reading on the subject of calendar changes over time**.**

Having established my ground rules for dating, I can now answer the questions – what about the apple tree and the Garden of Eden, and why did I choose 6000 years as a period of espionage history?

It is often said that prostitution is the oldest profession, but espionage – which includes covert activities and disinformation as well as spying – can be traced back to the Garden of Eden. Of course, 6000 years is misleading because scientific research recently used DNA of a lock of aboriginal hair to prove that Aboriginals reached Australia some 75,000 years ago, in the first major migration from Africa.

However, my late mother's Bible, presented to her in 1912, states that everything started in BCE 4004, hence my 6000 years.

A recent series on TV showed that the Bible was not written in one specific year or in a single location, but is a collection of writings, and the earliest ones were set down nearly 3500 years ago. The first five books of the Bible are attributed to Moses, who lived between 1500 and 1300 BCE. Some events he recounts in the first eleven chapters of the Bible occurred long before his time, such as the creation and the flood, and came from accounts handed from generation to generation in songs, narratives, and poetry. There is a 500-year period when no writings were contributed to the Bible at all, when Alexander the Great conquered much of the world and when the Greek language was introduced to the

Hebrews. The New Testament was written during a much shorter period, in the last half of the first century Common Era.

In looking at all these dates, when the Bible was written is not as important as what was written.

At the back of my mother's Bible is a list of many of the words used in the Bible, and where they are to be found. This list is known as a "*concordance." "Spy"* is listed a number of times, but "*harlot"* and " *prostitution'"* are not listed because they rarely appear.

I begin my search for the origins of espionage with **Genesis 3,4**: "***God creates man, and eastward in Eden, a garden with the tree of life and the tree of knowledge of good and evil."***

God was thoughtful enough to create Eve as company for "*man'",* but warned Adam not to eat the fruits of the tree. I am not sure how Michelangelo (1475-1564) received the message – perhaps a vision – but when he painted "Temptation and Fall" on the ceiling of Sistine Chapel in Rome he showed the serpent with a female body.

Figures 1.5 and Fig 1.6 The Garden of Eden and Adam taking the Apple

The serpent was the first female agent, a provocateur, code-name SNAKE and assigned by the Devil to stir up trouble in the Garden of Eden.

Genesis 3:6 records that the serpent convinced Eve to try the forbidden fruit, but an intelligence analyst – a burrower – would detect some disinformation as the enlargement shows Adam reaching for the apple while SNAKE is restraining Eve's fingers.

Whatever the interpretation, God put a curse on all serpents. **Genesis 3:14** – "*upon thy belly shalt thou go, and dust thou shalt eat all the days of thy life."* That curse still haunts intelligence agents.

Did you know that the Devil has a code number? The Revelation of St John the Divine **– 13:17 & 18** – refers to the Devil as the beast with seven heads and ten horns, and says: "*His number is six hundred three score and six."* If you do the sums you'll find that **600 + 3*20 + 6 = 666 = triple six.** People who have a fancy for things mystic see that number as dangerous and breathed a sigh of relief when 6 June 2006 passed safely = 060606.

Reference

***www.people.com/people*/archive/article/0,,20064457,00.html – Victor Marchetti**

***https://en.wikipedia.org/wiki/Peter_Wright,* Anna Chapman – Wikipedia**

***Samuel Morse & Morse Code* - Wikipedia, *Michelangelo (1475-1564)* – Wikipedia**

Next

In the next unit we will look at how espionage developed from the times of the Bible to 1400