Some Human Factors in Codebreaking

Christine Large
Trust Director, The Mansion
Bletchley Park MK3 6EB
UK
Tel: Bletchley +44 1908 647269 London +44 207 737 7220 Mobile +44 7971 193546

E-mail: christine@christinelarge.com

Christine Large, who has been Director at Bletchley Park since 1998, describes how human ingenuity and in particular, the Poles' early contribution, led to breaking a seemingly insoluble problem – the Enigma machine. She will speak with reference to Dillwyn Knox's seminal meeting with Marian Rejewski and the collaboration between men and machines that flowed thereafter. Some human factors that can lead to vital 'breaks' are highlighted. Bletchley Park's current rôle in Anglo-Polish diplomatic relations, including a joint public information campaign instigated as a result of the film, 'Enigma', is explained.

INTRODUCTION AND HOW HUMANS CREATE SECRET MESSAGES

The odds of winning the jackpot in the UK's national lottery are calculated to be fourteen million to one. The odds against cracking the Enigma code make that look like a safe bet. In simple terms, the dice are loaded one hundred and fifty million million million against.

For the purist, Enigma is not a code, for a code works by replacing a whole word or phrase with letters, numbers or symbols whereas a cipher substitutes individual letters in a word. The approach to solving them can be very different, but the terms are often used interchangeably and making the messages themselves secret goes back as far as language existed.

Mesopotamian peoples in around 3300 BC developed a universal picture code – pictograms – to describe the world around them, as had the cave painters before them who left messages in paintings and simple symbols.

Central American Mayans in 300 BC combined whole ideas and sounds into what we call 'glyphs', representing numbers with dots and bars. Their meaning was undiscovered till 1980.

The Aztecs who ruled what has become Mexico from the 1200's also used complex pictures and symbols to record time's passage. Experts have still not discerned the meaning of one, four thousand year old, sophisticated Indian script.

Hieroglyphs were an Egyptian system in use between 3100 BC and 600 AD, but it was not till centuries later that the ancient language revealed its secrets. At the very end of the eighteenth century, the Rosetta stone was discovered in the Nile delta. Weighing three quarters of a tonne, the black slab was chiselled with text in hieroglyphs, demotics, the business language of Ancient Egypt's scribes and in Greek – which was to provide the crucial 'crib' or way in to the message. Champollion, a Frenchman who had been a child prodigy,

Paper presented at the RTO HFM Symposium on "The Role of Humans in Intelligent and Automated Systems", held in Warsaw, Poland, 7-9 October 2002, and published in RTO-MP-088.

had prepared himself for the attempt by learning twelve ancient languages. Eventually, by studying sets of inscriptions in different languages, he found one common letter, deduced that vowels had been omitted and found that the hieroglyphs, representing sometimes whole words, sometimes letters, started to make sense to him. His mental abilities foreshadowed those of Dillwyn Knox, a prominent Enigma codebreaker.

Another innovative method of secret communications, according to Herodotus, a chronicler of 5th century BC, had been to shave a messenger's head, write the message on the head and dispatch the messenger once the hair had grown back. This is a branch of secret communications called steganography, which translates as 'covered writing.' Alongside steganography, a form of message protection called cryptography (from the Greek for 'hidden') evolved, whose intention was to conceal the meaning of the message, not just the message itself.

One of the world's greatest generals, Caesar, was using ciphers regularly in the first century BC, as revealed in his chronicles of the Gallic Wars. The occasional method of delivery, such as attaching the message to a spear, might be unconventional, but he was a classic cryptographer, substituting letters in a text according to a system that allowed the recipient to decipher the message without the enemy being able to read it. Julius Caesar invented his own cipher, substituting one letter for another – a technique that Enigma was to take to unprecedented lengths many centuries later.

There are many reasons why the need for secrecy has caused message senders to conceal their intent and message recipients or interceptors to wish to reveal what is concealed. Kings, queens, the military, security forces, politicians and businesses had discovered the advantages of systematically keeping messages and information secret but without doubt, the prime motivation for doing so was the presence or threat of an enemy.

In the sixteenth century, a legendary spymaster and a father of modern cryptography served Her Majesty Queen Elizabeth I. Sir Francis Walsingham was in the first rank of Elizabeth's ministers. He was ferociously bright and ruthless, which he needed to be in order to protect the queen's security. Arguably the forerunner of MI6, the UK's overseas intelligence agency, Walsingham had established a network of foreign agents to send him information from enemy territories abroad, where anti-royalist conspiracies often originated. He operated from over thirty locations in continental Europe, as well as Constantinople, Algiers and Tripoli.

Occasionally, steganography and cryptography combined, as when German agents in World War II scrambled messages, condensed them to the size of a dot and hid the information in regular text. Recently, details have come to light about terrorist groups that have been using the internet, an 'open' medium, to conceal secret coded information in familiar places such as digital paintings. The enemies may have mutated and changed their ground, but the need to preserve and uncover secrets is very much alive in our society today, whether for military reasons, or in daily situations that affect us all, like ensuring the integrity of financial transactions.

Keeping information secret by concealing it has existed just about as long as humans have, with endlessly ingenious devices to achieve the desired effect. I am going to select one particularly well-known device and briefly illustrate how 'breaking' it led to a revolution in secret messaging and in collaboration between men and machines. I will also allude to the feelings and behaviour of some of the key people involved and to human consequences that can flow from decisions about code making and breaking and indeed, how it is portrayed.

ENIGMA AND ITS DEFENCES

It was in the financial sector that Enigma started its life, far from the battlefields of Western Europe that would be Enigma's eventual arena. Arthur Scherbius, an electrical engineer, was trying to sell his wares. He had designed Enigma for the banks, for which transaction security and retaining the lead in security issues are abiding issues and business drivers. In April 1918, Scherbius wrote to the Imperial German navy saying he had applied for a patent for a cipher machine. Scherbius claimed he had invented a wholly new system of cryptography, embodied in his electrical Enigma machine.

The machine was based on rotors, wired codewheels made of nonconducting material. Evenly spaced around the circumference of the disk on both sides were electrical contacts, usually 26, usually made of brass. The contacts on one side were connected to those on the other side by wires through the body of the rotor in a random arrangement. Each contact represented a letter, so the rotor was a 'coded' alphabet. To encipher a letter the operator pressed the appropriate key on the typewriter-like keyboard, so completing an electrical circuit into the rotor at the corresponding input contact. The circuit continued through other rotors to a different output and on to a light bulb, which showed the letter as the enciphered version.

Electrical encipherment was not in itself revolutionary. Scherbius's innovation lay in the machine's wiring and the ability of its wheels to rotate. Imagine a type of infinite electronic pinball, where the ball is a current whizzing unpredictably along tracks and it eventually pops up in a random pocket.

The genius of the rotors was that when a rotor reached a certain position, the rotor on its left would be turned, individually or in groups, effectively altering the routes through which the electrical impulses would pass from the key before arriving at a bulb and dramatically increasing the encipherment options. Therefore, the machine's most important characteristic was that, if the operator pressed the same key on the keyboard over and over again, a random series of letters lit up on the glass panel. The original letter was randomly scrambled through the internal wiring, making it almost impossible to predict what the enciphered letter would be, or to work backwards from an enciphered message to the original text. After one analysis of Enigma's defences, a German cryptographer wrote, "…due to the special procedures performed by the Enigma machine, the solvability is so far removed from practical possibility that the cipher system of the machine, when the distribution of keys is correctly handled, must be regarded as virtually incapable of solution." The incredible number of ways to set the keys and the machines convinced the Germans who used it in the Second World War that Enigma was invincible.

Germany in World War I saw no reason to believe that its codes had been jeopardized, lacking sufficient, as they saw it, anecdotal information or compelling facts. The effect of admitting that the enemy might have broken German codes would have been to compound the military's sense of inertia and unwillingness to face reality, for it would have required battle plans to be changed and a complete overhaul of codes, planning, administration, security and personnel. It was not a prospect that the Germans seriously contemplated and it was an arrogant mistake that would be repeated in World War II.

GERMAN SECRET MESSAGING PROCEDURES

A message would often start its journey from land and might begin with a senior command officer or close subordinate writing it out. The watch officer took the message to a command transmissions officer, whose job was to stamp it with the time and pass it on to a radioman, who began the enciphering process. Radiomen were responsible for enciphering, transmitting, receiving and deciphering radio messages and they commonly had access to a bank of several Enigma machines.

The radioman took the message and pressed it out key by key on the keyboard. A colleague wrote down the enciphered letter that appeared as a different, illuminated letter behind the keyboard. The message was written down in four letter groups, with two, four letter 'indicator groups' at the beginning that were copied at the end. The message was annotated with a date time number, a number stating how many four letter groups the message contained (not counting the indicator groups repeated at the end) and it was given a serial number.

An error in the enciphered text would have produced a nonsensical or misleading result when it was deciphered. Another radioman therefore did a dummy run of the procedure that the receiving radioman on a U-boat would follow. If the message did not decipher correctly, it was corrected.

The radioman's next task was to choose the radio network on which to transmit and the frequency that he used within the network, depending on the time of day. There were networks based on geography, on legend and on history. The names were often chosen to inspire a feeling of prowess and good fortune, for example, invoking by implication the powers of 'Diana', Greek goddess of hunting. The radioman turned his radio to the frequency and tapped out the enciphered message in Morse code, a series of aural dots and dashes. These signals were relayed by wire or pumped through the airwaves by relay stations and could be repeated several times.

Automation, of course, is supposed to improve capability and in the case of Enigma, optimise security. The machine was designed to do as much as possible from an efficiency point of view, leaving theoretically no need to exercise human judgment, especially when it came to randomising letter selection. The machine was 'in charge' as much as possible. But think about the operating and operator conditions.

ENIGMA OPERATING CONDITIONS 'IN THE FIELD'

From the comparative comfort of command control, the message sped to a player on the chessboard of war, perhaps a U-boat in the North Atlantic. U-boats could receive messages up to forty feet down and the receiving radioman would be stationed in his cramped office, in the bowels of the ship cocooned by the inky deep. Medium height, mentally tough and physically wiry, he had volunteered for submarine service, liking the independence and the responsibility. Hunched at the desk, able to touch all four walls from his seated position, he would be temporarily oblivious to the sounds and scents that infiltrated every aspect of life on board. Fetid, stale air clung to every surface if the ship had been submerged for some time as it moved towards a target, skirting enemy occupied sea and avoiding surveillance. The unsleeping engines resonated in the background, a low vibration that set teeth on edge, drilling through the Atlantic's salted dark underbelly. Yesterday's dinner wafted from the galley, mixing indiscriminately with human sweat, condensation and machine oil odours in the submarine community.

Mr. Radioman blocked it all out, clutching earphones to his head, closing his eyes and concentrating on extracting the Morse signal from a mass of white noise hissing through the air. The ship juddered and his books crashed to the damp metal floor. He was hot, exhausted, hadn't eaten because he had been expecting the transmission, always on vigil. Serial numbers told him if he had missed any messages. Negligence was punished, but sometimes a message could not be received because the U-boat was too deeply submerged. The radioman had committed the enciphered message to paper. His Enigma machine had been set up mirroring the procedure at command control, according to the instructions of the day. He set about deciphering it, translating a letter of Morse to the typewriter – it required some pressure to depress the stiff keys – and backwards the signal span through the rotors and plugboard, finding the right exit at the illuminated panel and ending that stage of transit in the original 'plaintext', the unenciphered message that originated at its German author's hand. A convoy contact report; top priority.

He pushed himself up from his hard stool, closed the wooden lid of the Enigma machine, switched off the reading light suspended on a cord over the tiny desk, eased stiffly out of the narrow door, which he locked and hurried to his captain with the deciphered message. It might have been a routine weather report, another short transmission, headquarters could have been establishing a key, or a rendezvous with a submarine carrying fuel for the boat, the message might not have been for his particular boat, but this time… they would be seeing action.

What aspects of the human factor might manifest themselves here? A radioman in a submarine or, perhaps, under fire or the threat of it, would be prone to forget rules and procedures, would suffer from time pressure, might lapse into inattention through fatigue or stress, or have a breakdown of skill; factors that the codebreakers and allies of Bletchley would, in due course, rejoice in exploiting.

THE POLISH SITUATION

Perhaps more than anything, codebreakers dread silence, the absence of comprehensible communications when they cannot tell if reinforcements lie a hundred miles away, or they are a step from the deepest abyss. Often, that silence is broken by intuition and luck as much as by intellectual prowess.

One nation that could not afford an intelligence blackout was Poland, for Germany was a river's width away, poised aggressively on the border. With self-interested foresight, the Poles founded a cipher bureau in 1918 and started to monitor Germany's activity through its coded messages, which they were able to read from the outset until 1926. In that year, the Poles noticed a change in German cryptograms that they deduced to be attributable to the introduction of machines.

There was a curious incident in Warsaw's customs office around the end of 1927 when a package labelled 'radio equipment' turned up due to what the sender's German representative described as a 'shipping mistake'. The German insisted that the package be returned without being opened, but not before the cipher bureau had identified it as a potentially interesting cipher machine – not a transmitter/receiver. Among Enigma inventor Scherbius's first customers must have been the eager Pole who purchased a commercial Enigma for the Polish cipher bureau, maybe not realizing that it could not decipher military messages. The analysis of mechanized codes after World War I could not depend on word and code based linguistic techniques. New thinking was required to deal with the ciphers being generated by Germany's secret servant. The first machine enciphered military messages were intercepted in July 1928.

German-speaking mathematics students were sought to solve the machine and one of their number was Marian Rejewski, a promising young man aged twenty-three. Rejewski had attended a cryptology course run by the cipher bureau at Poznan University. He was deputed to work alone on breaking the Enigma cipher. He devised a set of equations to try to understand the significance of the six letters, the 'key' that appeared at the outset of an enciphered message, but it was a struggle to make the mathematics sufficiently simple to solve. For good measure, not wishing to overlook any clues to the fiendishly difficult puzzle before them, the Poles also called in a clairvoyant.

Rejewski was to discover that Enigma's Achilles heel was its opening three-letter message key, which was enciphered twice. Rejewski designed a grille to test which rotor was in use and what its starting position was, moving on to discover where the alphabet rings had been set on the rotors. The plugboard settings were largely irrelevant and the Poles' attack on Enigma started to yield results. Some messages could be read on the same day and the Polish unit was geared up to deal with the increase in volume. Enigma replicas were used to

read messages and recover keys. As the German rearmament programme gathered pace, so did the message volume and rhythm of rotor changes.

MACHINES INCREASE PROCESSING CAPACITY

Machines were invented to provide additional capacity. The cyclometer, an electromechanical device linking Enigma rotors was useful in recovering rotor orders and settings. An ice cream sundae called 'bomba' 'baptized' the 'bomby', a parallel processing machine inspired one day over dessert. Rejewski's process harnessed six Enigmas to try multiple rotor orders. A correct bomby 'stop' produced text.

In December 1938, a new silence descended. Enigma messages became indecipherable because the Germans introduced a choice of five rotors, not the original three. Two of the rotors' wiring was unknown, but at this stage the Germans did not change their method of enciphering the message key and the ingenious Poles again reconstructed the rotor wiring using their tried and tested methods. Plugboard connections escalated to ten in January 1939. The Poles would have needed ten times their processing capacity to crunch the number of permutations.

Tension between Poland and Germany stretched their relations to snapping point and once the French had agreed to attack Germany promptly should Poland be invaded, the Poles unilaterally resolved to share their Enigma revelations.

A SEMINAL MEETING

The Pyry forest (something of a misnomer as, whilst it has trees, it is heavily populated with buildings) was the venue for an historic meeting hosted by the Poles for the French and British in July 1939. Bletchley Park director Commander Alastair Denniston, Dillwyn Knox and Commander Humphrey Sandwith travelled the ten kilometres from Warsaw to Pyry with the Polish cryptographers.

Imagine the astonishment when the Poles revealed their Enigma replicas and showed their allies the six bomby. It was like being given the key to a treasure chest. The Poles were unstinting with their knowledge and handed over, in the days after preliminary discussions, heaps of decrypts, Zygalski sheets, the principles of their bomby and, to top it all, one Enigma replica each for the British and French.

Although, as Rejewski recognized, Dilly was close to breaking German Enigma when they first met, the order in which the typewriter keys and lamps were wired to the entry plate had proved intractable. The Germans were not using a QWERTZU diagonal and Dilly had assumed that the letter order would be random to compound the difficulty. He was wrong; it couldn't have been simpler and he was rendered speechless to discover that the running order was ABCDE. The Poles had made a model with an ABCDE keyboard for their own use. A letter of Dilly's unearthed by historian Dr. Ralph Erskine confesses that a certain Mrs. BB at GC&CS had been ignored when she made the very same suggestion.

Marian Rejewski spoke, in 1978, of the immediate rapport between him and Dilly, "Knox grasped everything very quickly, almost as quick as lightning. It was evident that the British had been working on Enigma so they didn't require explanations."

The Poles then, through Rejewski, carried the honours for first reconstructing Enigma's wiring and working out a method for finding its message keys. The Polish contribution in making these inroads was not to

be officially recognized until sixty years after the event, in an anniversary celebration at Bletchley Park on 25th July 1999.

A CODEBREAKER IN EXILE

The Polish 'Biuro Szyfrów' (Ciphering Bureau) had been operating for several years, showing, according to Rejewski, "…results which other nations such as England or France could only dream about." Each month, the bureau had passed on thousands of broken messages from German military, air, navy or SS sources.

With the outbreak of war, or even a few months before, the period of excellence declined and three principal Polish mathematician-codebreakers, Rejewski, Zygalski and Rozycki were deprived of the opportunity to exercise their full abilities. The reasons for this, which I will cover, were political and security issues but the human factors in codebreaking had a strong bearing too. Thanks to Eugenia Maresch, archivist at the Polish Institute and Sikorski Museum in Great Britain, I am able to share extracts from Rejewski's papers that disclose his state of mind.

'Kilka uwag na temat trudności w jakich znajuje się chwili obecnej Dział szyfrów niemieck' *A few comments on the present difficulties which the Polish section of German ciphers is encountering:*

"During the French campaign the Polish analysts were assigned to the 'Bureau de Chiffres'. Instead of concentrating on research, they were dealing with ordinary traffic, a task which could have been done by the general office staff…After the fall of France [June 1940], the cryptological work was performed under conspiracy…"

The background is that the British government was reluctant to co-operate with the Bureau because of the ambiguous Vichy government. A memo, classified at the time, asks, "We must ask them [the Bureau]: – Who are their masters (i.e.) If they are officially paid by a Government which may join the Nazis at any time, it is too risky for us." Too close a collaboration could have resulted in losing the entire Ultra operation and possibly, WWII.

When France was overrun, the 'Biuro Szyfrów' had to be liquidated and all materials, instructions and a replica of an Enigma machine were hidden in a secure place. Some Polish cryptanalysts were arrested and went to German prison camps. Rejewski and Zygalski managed to reach England. They resumed work at the Polish Research Centre in Stanmore and Boxmoor – not at Bletchley Park.

The British recognised, in a secret memorandum that, "…without this liaison with the Poles, arranged by the French, we might not have been able to break [Enigma] in 1939 and thereafter establish daily contact." On January 9th, 1940, the then Director of Bletchley Park, Commander Denniston, wrote to his head of service saying, in respect of the three Polish cryptanalysts, "If we are faced with a change [in Enigma] on the outbreak of war (and we begin to suspect it), the experience of these men may shorten our task by months. We possess certain mechanical devices, which cannot be transferred to France. These young men possess ten years' experience and a short visit from them might prove of very great value."

Rejewski, writing in 1944, was of course unaware of the British arguments and he found his isolation from top-level cryptanalysis, deeply painful. "It would be fitting to remind the English that they owe a debt of gratitude to the Polish Cyphering Bureau…it is worth emphasising …what precisely the Polish cryptanalysts expect from their English colleagues. First, they should be asked to return the Enigma machine which was given to them…Subsequently one should enforce an agreement so that they would share their experience on

German ciphers…Lastly, one should try to persuade them to pass on the intercepted traffic material. This would be helpful as the Polish possibilities are very limited." Rejewski was grateful for the, "exceptional hospitality on French soil" and referred to, "a personal bond of friendship" but he recognised that, "while the French co-operation would produce results at a later stage, the Anglo-Polish joint effort would show results almost instantly."

PREPARATIONS FOR BRITISH BREAKS INTO ENIGMA

So just how were the British obtaining some of their results? Common misconceptions are that the Bletchley operation was either a handful of chaps in a wooden hut, or that machines, especially Colossus, the world's first semi-programmable digital computer, produced the answer. The answer was neither and both.

Bletchley did build up very rapidly indeed from the small beginnings initiated through 'Captain Ridley's Shooting Party'. Wooden huts proliferated in November 1938 to house the now highly productive Enigma decrypt teams. The first Bombe was in operation in August 1940, supporting Enigma breaks. Colossus 1 was a much later development. Working from December 1943, it was followed by ten others that were used to obtain the key to a sophisticated cipher used personally by Hitler and his High Command. The codebreakers, around 400, were at the core of a staff 12,000 strong on the Park. By 1944, Bletchley had an almost worldwide intelligence network. Decrypt stations in Malta, Cairo, Nairobi, Mombasa, Colombo and Brisbane were revealing enemy secrets, passing them on to operational theatre commanders and then sending them back to Bletchley Park for an overview of the war. Raw material came from thousands of wireless intercept officers in outstations – the Y Service and communications, especially Abwehr traffic, intercepted by the Radio Security Service. It was a huge, secret operation.

I'd like to take you back to the German radioman whom I described earlier, as he holds the clues to other human factors in codebreaking.

ENIGMA'S CHALLENGES

What made Enigma so difficult to break? The machines mustered a number of variable elements. In a typical, three rotor Enigma, the plugboard was at a right angle to the user, visible at the front of the machine when the wooden flap covering it was pulled down. It had the appearance of a flat metal plate, into which rivets had been punched. There were three, double-banked rows. By each plug hole was a letter, in the QWERTZU keyboard order, or a number. The twenty-six holes were designed to receive up to thirteen small, cylindrical metal plugs or 'jacks' sheathed in Bakelite type material. From each plug protruded a short, double-wired cable. When a cable was inserted, it could make a connection between any pair of letters. Each cable therefore used two holes to make the connection between letters. To calculate the plugboard permutations depended on how many cables were used, which group of holes was selected and the interconnections between these sockets.

Dr. A. Ray Miller has calculated the number of theoretically possible Enigma permutations by examining the maximum possible combinations for each component of a three rotor Enigma and combining the values. He said, "To see just how large that number is, consider that…there are only about 1080 atoms in the entire observable universe." The total of possible three rotor Enigma combinations is approximately 3 X 10114.

It is a number that has no meaning in daily existence. Bletchley Park codebreaker and Dillwyn Knox protégé Mavis Lever (now Batey) modestly avowed, "When we were breaking Enigma under Dilly's guidance,

thank goodness no-one explained exactly what we were doing. Had they done so, I don't know how we would have managed it."

Fortunately, the Enigma machine's practical operation and development increased the chance of penetrating these astronomic potential configurations from the frankly, impossible to the merely miraculous.

HUMAN FACTORS LEAD TO BREAKS

Human error and Enigma radiomen's characteristics and quirks prompted some great codebreaking successes. David Kahn reported an instance in 1932 when an operator who was supposed to delete codewords that were unenciphered, crossed out the enciphered ones instead and transmitted the message in plain text. Aghast, he reported his mistake, only to have it foolishly compounded by an order to retransmit the message with the correct, enciphered words. Anyone listening had the complete Enigma version, translated in 'clear'. Following this incident, the navy fortified and sharpened up its training, as well as changing keys.

Choosing keys that were easy to remember was a tendency first spotted by Rejewski. Girlfriends' names, personal initials and imprecations topped the user poll. Mavis Lever claims only half in jest to have been a world expert on wartime dirty four-letter German words! These foibles in Enigma message settings were named 'cillies'. Less frequently, the Germans 'blew' what were called 'kisses', by repeating parts of Enigma messages in a vulnerable cipher. Mavis Lever said, "As soon as I picked up one long message I could see that it had no L in it; as traffic was so infrequent operators were told to send out the occasional dummy message and this one had just put his finger on the last key of the keyboard, probably relaxing with a fag in his mouth." The sloppy operator had used L to encipher the whole message, giving the cryptanalyst the new wiring for the Enigma rotor.

HERIVELISMUS

Another great coup became known as the 'Herivel tip', although John Herivel refers to it as 'Herivelismus.' Gordon Welchman had been Herivel's supervisor at Cambridge and it was his former supervisor who invited him to Bletchley in 1940, "to do some very important work." Herivel said, "One thing I was very clear about in the beginning was, that it was much more likely to happen if the German operators were working under great stress. They were more likely to make mistakes if they were frightened, in a great hurry or very tired." Herivelismus was inspired by an intuitive leap that put John Herivel in the shoes of the German operator. Herivel visualized the German sitting there, with the wheels and the book of keys. After he found the right wheels for the day, loaded them on the sprung spindle, fitted them into the machine and clicked the rotors round to the day's setting, his next task was to choose an indicator. What if the operator were afraid, in a hurry or distracted? Might he just bang down the hood, see the letters showing under the window in the top and use those? How did he actually deal with the ring settings? Rather than having set them, as he should have, at the outset, perhaps the anxious or lazy operator would set them after he placed the wheels in the machine. In that case, the indicator letters he chose as his message setting for the day would surely be close to the ring setting. It was an inspired guess whose net effect was to narrow down the 17,576 possible ring settings to maybe as few as twenty. Herivel remembers very clearly that his 'Tip' worked properly for the first time on May 1st 1940.

Welchman's thanks to Herivel was to ensure that Winston Churchill subsequently singled John out. In 2001, at Bletchley Park, Herivel reflected on his discovery, "…and when I thought about that more I realized the really vital move, was for me to want to find some new way of breaking Enigma. It was very strange as

I'd only been there for three weeks and only just got to know under the instruction of Turing and Kendrick how the machine and the system worked."

Intercepting and analyzing the traffic, the formidable permutations, the cryptographic security, the stringent procedures; for all these reasons, some variations of Enigma were strongly resistant to being broken. Yet while human resourcefulness could create awesome complexity and brilliant cryptanalytic inroads, it was the human factor that rendered Enigma most vulnerable. A formidable machine, both designed and undermined by humans.

AUTOMATING CODEBREAKING AND WORKING WITH MACHINES

Bletchley moved the design of bombes into a new league, in particular with Welchman's innovative diagonal board. The IEEE, an American organisation of electrical and electronic engineers, is shortly to unveil a plaque at Bletchley, commemorating it as the site of the world's first electronic codebreaking. However, it was the Americans who developed a machine designed to deal with four rotor Enigma and capable of being mass-produced.

The American testing machines were bigger than their British cousins, weighing about two-and-a-half tons and they ran much faster. The Bombe Room at Bletchley had been known as the 'Hell Hole'. In Dayton, large air conditioners were installed every ten feet and the American bombes ran twenty-four hours, seven days a week.

'Grey elephants', as they were called, lined the rooms, lumbering six feet high, three feet deep and ten feet wide. The operators were given charts that explained how to set the rotors and switches on the machines, thirty-six of each. The bombes' accuracy relied on the efficient women hand-picked to run them. "We worked in ungodly hot buildings with those machines," said Beatrice Dunphy. "Salt dispensers were near the water fountains. And the noise was terrific…"

By mid-1943, the American and British cryptanalysts had become so proficient at finding cribs, due to their familiarity with German naval signals, that naval Enigma was almost an open book. The availability of bombes at last matched the abundant cribs. As cipher machine complexity escalated (high-level machines were anyhow used by the German commanders), the British responded by inventing the first computer. Colossus was based on valves rather than relays, designed by Post Office engineer Tommy Flowers responding to the principles of Turing's universal machine. Colossus, like the bombes, was a tremendous advance but both machines were, in a sense, mere number crunchers supporting human judgment and intuition in the codebreaking process. The bombes required relays of humans to set, run and maintain them and Colossus, once it started, needed to be kept running – they were the first of their kind. I suggest that the scale of Bletchley and the Allies' phenomenal achievement, commonly considered to have shortened WW2 by two years, was surely only possible because men and machines were working in harmony, playing to their respective strengths.

A COMMUNICATIONS REVOLUTION

At first glance, realizing the odds against reducing possible combinations of Enigma keys to discernible messages should have stopped any attempt to do so in its tracks. From discussions I have had with former codebreakers, the 'attack' on the problem starts with total intellectual immersion in it, the 'left brain,' assembling disparate information. Then the mind starts to relax and lateral 'right brain' thinking kicks in,

which is when solutions start to appear. At first, the problem can seem repellent, like an impenetrable crossword clue, but as the next clue emerges, it becomes obvious what the previous piece is.

Codebreakers are looking for pattern recognition, something that the human brain is incredibly good at and computers are not. Bedazzling short cuts are ways of destroying randomness by seeing patterns – linguistic, numerical, pictorial, spatial and combinations. Being methodical is the worst possible approach. Compare the 'brute force' original bombe design, crunching through sequences to help determine whether cribs could be used to decipher Enigma messages. Welchman's insightful diagonal board made the bombes more efficient at a stroke by chopping down the number of combinations to be tested. Take Turing's approach to codebreaking, which he likened to finding a needle in a haystack. Method would suggest that the haystack should be divided into equal segments and searched. Turing would have thrown away each piece of straw until he found the needle. "Which way round does a clock go?" asked Dilly Knox. Clockwise – the methodical answer – is wrong, if you are the clock.

Cipher machines and the technology required to break them were at the heart of a communications revolution engendered by the Second World War. Warring countries competed for technological supremacy, pitting their finest scientific and engineering resources against each other. The results were to have an impact far beyond the immediate arena and nowhere more so than in the field of secret communications, where the latest information on advanced planes, submarines, weaponry and defences was for the taking.

BLETCHLEY AND ENIGMA BECOME LEGEND

Michael Apted's film of the Enigma novel, released in the UK last year, ended with panache. The problem was that unlike the novel, it didn't quite make sense. Tom Jericho, the reclusive codebreaking hero in Robert Harris's novel enters the film having been recalled to Bletchley Park after suffering a nervous breakdown. We learn that the cause is not, as did happen in the real wartime Bletchley, the intense intellectual pressure of generating solutions to almost impossible problems. Jericho collapsed from unrequited love for Claire Romilly, a bright and mysterious femme fatale who, to paraphrase her room mate Hester, Romillies her way through the Park's susceptible males at a prodigious rate. Claire disappears from Bletchley at the same time as Bletchley's ability to read key German U-boat codes is lost and there are suspicions of skulduggery. Jericho uses his return to the Park as a cover for the quest to protect Claire. By the end of the film, the miraculously restored and physically slight Jericho makes an astounding trip to Scotland, travelling without official sanction or apparent petrol coupons, whose pièce de résistance is a daring chase across a channel where an absconding Pole is set to reveal Bletchley's secrets to the German enemy.

"The Polish Ambassador is on the phone for you," said my PA. The ambassador was exceedingly exercised by the treatment of Poland and the Polish contribution to breaking Enigma in the forthcoming film.

There were no Poles working at Bletchley Park, as Rejewski poignantly stated and the poles were understandably upset that a Pole had been portrayed as the traitor willing to give away Enigma secrets, especially when so much of the rest of the story seemed to be true.

ENIGMA DIPLOMACY

To mark the 60th Anniversary of that historic rendezvous, and to give thanks for the Polish contribution to the cracking of Enigma, Bletchley Park had hosted a Polish Festival in July 1999. This has become an extremely popular annual event, with large numbers of Anglo-Polish and British people from all over the country

coming to Bletchley to join in the celebrations. A few days prior to the 2000 Festival, a special ceremony took place at the Palace on the Water in Warsaw. The families of the three outstanding Polish cryptanalysts were presented with the Great Cross of the Order of Polonia Restituta (Poland's Rebirth) by Polish Prime Minister Jerzy Buzek in recognition of an achievement that many consider to be Poland's single greatest contribution to the Allied victory in WWII.

In September 2000, it was Britain's turn to present an Enigma machine to Poland. On an official visit to the country, HRH The Duke of York presented a machine to Mr Buzek as a "symbol of Britain's gratefulness and thanks".

As Enigma – the film – was launched, Bletchley Park engaged in a round of diplomacy involving public lectures, speeches, meetings and publications. At our joint conference in September just past, with Christ Church, Oxford, Professor MRD Foot gave a paper on the Polish contribution to breaking Enigma.

The 2001 Polish Festival saw the unveiling of a commemorative monument at the Park, inaugurated by Bletchley Park's chief patron, the Duke of Kent.

THE CODEBREAKERS' HUMAN AND TECHNOLOGICAL LEGACY

In transformational times it is easy to neglect the aspects of our past that must be preserved to carry us into the future. NSA Director General Hayden said at a meeting in 2002, "It is very difficult for us to talk about the today equivalent of what is going on at Bletchley Park, but by talking about Bletchley Park we build up the kind of confidence and put the human face on the agency that we need in the national debate about us and our tradecraft…We need to be reminded what represents the best of us and to emphasize those things that do not much change."

US Deputy Secretary of Defense Dr. Paul Wolfowitz said, in testimony September 19 2002 to the Senate and House Committees on Intelligence, quoted Thomas Scelling,

"Surprise, when it happens to a government, is likely to be a complicated, diffuse bureaucratic thing [*how different to Bletchley Park*]…It includes gaps in intelligence [*Ultra's role*], but also intelligence, that, like a string of pearls too precious to wear, is too sensitive to give to those who need it [*think of Rejewski*]… It includes the unalert watchman, but also the one who knows he'll be chewed out by his superior if he gets higher authority out of bed [*remember the Enigma operators*]"

Dr. Wolfowitz spoke of Bletchley, saying,

"During World War II, the United States and Britain assembled their best minds to crack the German code. These codebreakers, assembled at a place in England called Bletchley Park, defied the odds, accomplishing their vital mission faster than anyone expected. In doing so, they hastened the demise of Nazi Germany and the end of the war. As we seek to defeat terrorists and their supporters, our intelligence culture must renew the sense of urgency in collecting and mining and analyzing intelligence that inspired the codebreakers of Bletchley Park."

Bletchley Park has a mission today, too, to build on the work of the wartime pioneers through a strategic plan that we have made good progress in implementing. Yet its future is not secure and Churchill's famous exhortation, when faced with a plea from Turing, Milner-Barrie, Alexander and Welchman, comes to mind, "Make sure they have all they need in extreme priority."