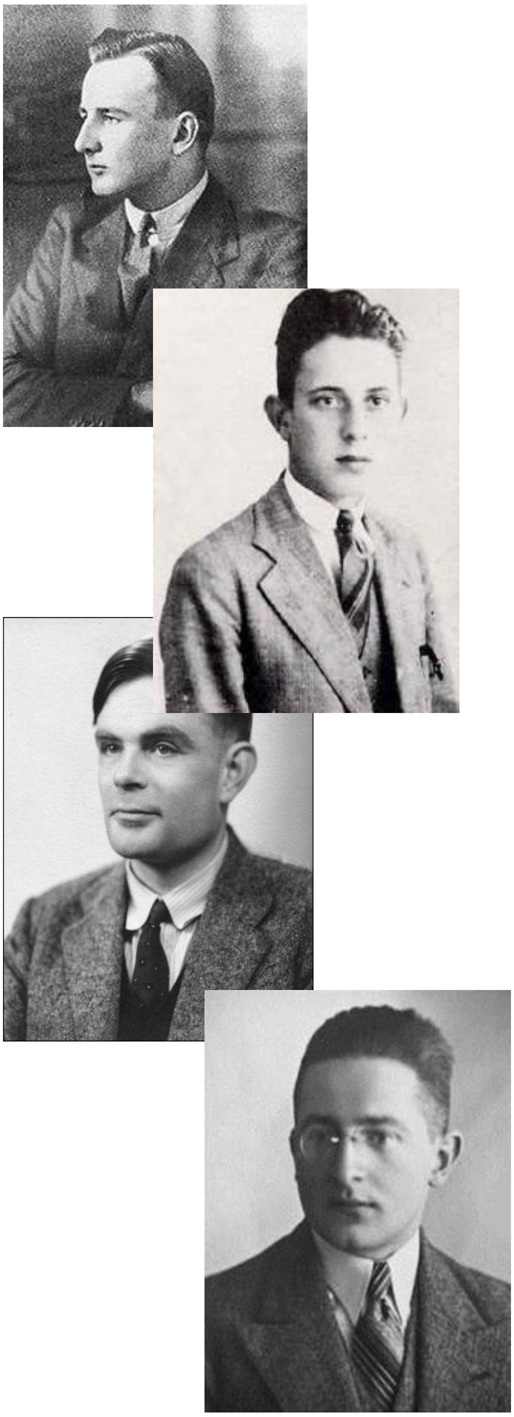
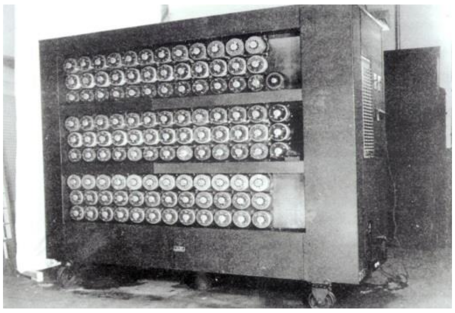
Did cracking Enigma define the Allies’ victory?

How crucial was the Enigma to Germany in World War Two?

Was this the most important reason that contributed to the defeat of the Axis?





Contents

Chapter One: Creation of the Enigma …………………………………………………….. 3

Chapter Two: The Polish Breakthrough ………………………................................. 4

Chapter Three: Bletchley Park ……………………………………………………….. 5

Chapter Four: The British Bombe ……………………………………………………. 6

Chapter Five: Top Secret Ultra ...…………………………………………………... 7

Chapter Six: The American Bombe ………………………………………………... 8

Chapter Seven: The Aftermath ……………………………………………………….. 9

Chapter Eight: British Intelligence in WWII ……………………………………………. 10

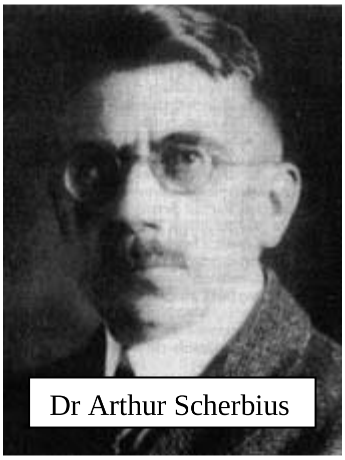
Chapter Nine: German Intelligence in WWII …………………………….................... 11

Pros and Cons of the Bombe ………………………………………………………….. 12

Conclusion ………………………………………………………………………….. 13

Bibliography ……………………………………………………………………..... 14

Chapter One: Creation of the Enigma



Dr Arthur Scherbius

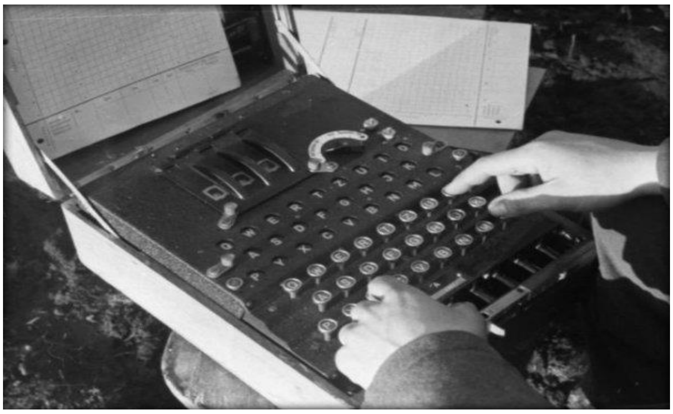
The Enigma was an electro-mechanical wired enciphering machine that came with a series of drums or wheels, which was used in World War II and created by a German engineer called Dr Arthur Scherbius.

The machine would enable an operator to type any message, and then scramble it using three to five wheels, or rotors, that displayed different letters of the alphabet. The receiver of the message would need to know the exact settings of the rotors to decipher the coded text. The first models of the machine were slowly developed by the Germans and became more complicated for their opposition; experts would add variable inter-connecting plugs with electronic circuits between the keyboards and wheels, new rotors, and the resort to a variety of different ways of setting the Enigma to more frequent changes every day. Plug boards and interchangeable rotors combined, provided millions of possible settings to choose from, which the Germans thought made the Enigma unbreakable.

There was one development, that pre-dates the Enigma, and that is the invention of Theo A van Hengel and RPC Sprengler, two Dutch naval officers who produced working rotor-based cipher machines for the Dutch War Department in 1915, which was believed to be the base for the Enigma machine.

After the Treaty of Versailles in 1919, the Germans wanted to improve their compromised communications system from WWI and recognised the potential of the Enigma that was originally made for the market. Scherbius had made the Enigma able to transcribe coded information, but its sole purpose was to impress companies in secure communications. He started his own company in Berlin, 1923; Scherbius & Ritter of Berlin-Wansee, for manufacturing, and in 1926, the German Kriegsmarine (Navy Forces) created their own version, the Naval Enigma, followed by the Wehrmacht (Land Forces) in 1928, and the Luftwaffe (Air Forces) in 1933.

The machines kept on developing over the years, and in 1932, the final version was made, Enigma-I. Due to Scherbius' sudden death in 1929, the German Army had claimed exclusive rights to the machine, after replicas were being placed on the market, since the model was only supposed to be for the army. In the early to mid-1930s, the Germans were preparing for war under Adolf Hitler's orders, therefore, they started to order large amounts of the Enigma-I machines.

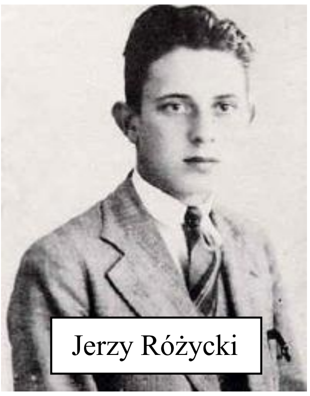


Chapter Two: The Polish Breakthrough

With Adolf Hitler running to become the Chancellor of Germany, the Allies first understood the problems posed by the Enigma machine in 1931 from a German double agent, Hans-Thilo Schmidt, known as Asché, who worked in the cipher branch of the German army. He allowed his French spymasters to photograph the Enigma operating manuals (Army Enigma Keys), in return for money, although neither the French nor British could at first make headway in breaking the Enigma cipher.

It was only after they had handed over details to the Polish Cipher Bureau, Biuro Szyfrów, that progress was made. They were the first to attempt breaking the Enigma cipher, as being one of the closest neighbours to Germany, they were very much aware of the likelihood of another war. From the University in Poznan, Poland, three young and brilliant mathematicians were recruited: Marian Rejewski, Jerzy Różycki and Henryk Zygalski. They started researching the commercial Enigma and, straight away, initiated working on the Enigma cipher, even with nothing more than a handful of intercepted messages and a description of the commercial Enigma.

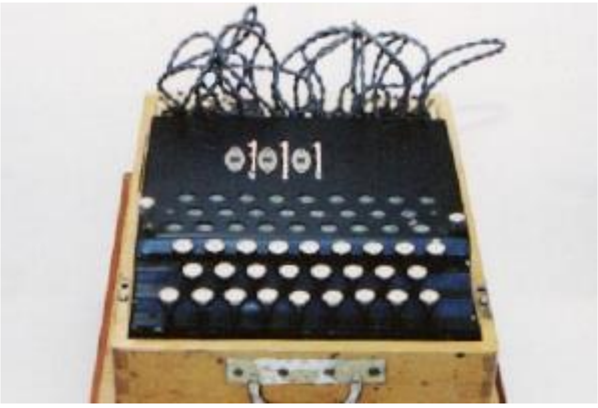
Marian Rejewski


Jerzy Różycki

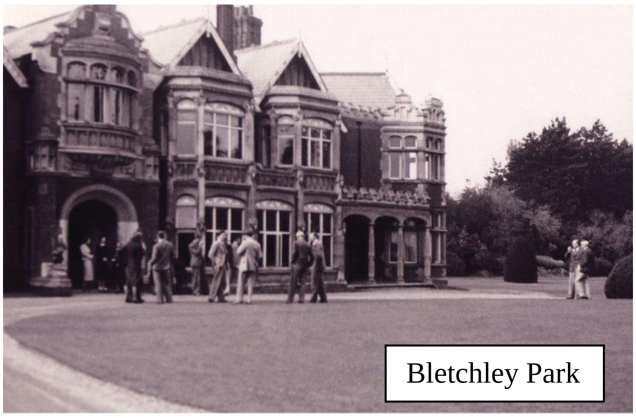
Henryk Zygalski

From 1933, the Polish Cipher Bureau had intercepted and decrypted a significant portion of the German's radio traffic. In 1938 they see an increase in the number of intercepted messages sent by the Germans, and from that day forward, it became even clearer that Germany were preparing for war. Unfortunately, by the end of 1938, the Germans had become even smarter, adding two new wheels to their Enigma machine, which multiplied the maximum number of potential settings by a factor of 10.

In the meantime, the Polish Cipher Bureau had built an equivalent of the Wehrmacht Enigma with a plug board added towards the rear. Rejewski later retrieves the wiring of the two additional wheels added and the suitably wired wheels are connected to the Polish Replica. With the war imminent, the Poles had started to look for ways to get their knowledge of the Enigma and the war out of the country before it was too late.



Chapter Three: Bletchley Park



Bletchley Park

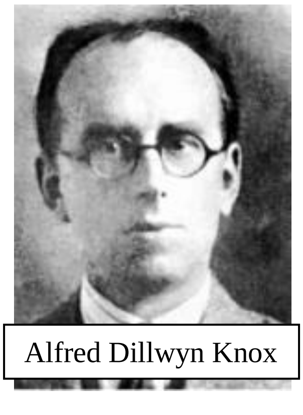
With the information in the hands of the main Allies, they needed experienced codebreakers to continue the work of the Poles and assist in cracking the Enigma code.

Alfred Dillwyn Knox was a codebreaker for Room 40 during World War One; he had been trying to break the Enigma code since he first found out about it in 1925, and had his first success in April 1937 when he broke Franco's Enigma K code. When Germany started to use the 'Steckered Enigma' for communication with Spain, he mounted an attack on its military Enigma, but was unsuccessful when working out its hardware. Yet, he managed to impress the Poles; they revealed their achievements and also gave Britain and France one of their replica machines, at a meeting in Poland. After the meeting, the Polish Cipher Bureau destroyed all of its documents and equpiment, whilst their cryptanalysists fled to France. A few weeks later, Bletchley Park was established and used for code breaking by the British.

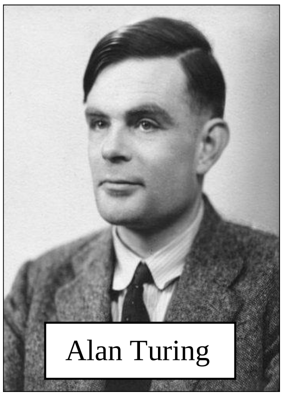
Whilst the Polish Cipher Bureau was still in contact with the British and the French, the Germans were planning their attack on Poland. On September 1st, 1939, Germany invaded Poland, but not before the Poles could get their understanding of the Enigma out of the country to Britain and France. Neville Chamberlain broadcasts two days later, September 3rd, 1939, that Britain and her allies have declared war on Germany and its allies, as they refused to withdraw troops from Poland. The Poles were interrogated about what they knew about the Allies and their upcoming plans, but they refused to give up their knowledge of what they discovered.

In the early stages of the war, the Poles continued to try to crack the Enigma code with the help of the French Cipher Bureau. Bletchley Park was an estate based in the small town of Bletchley in Milton Keynes, UK, the home of the GC&CS, Government Code and Cipher School, or the British Cipher Bureau. Bletchley Park was chosen because it had direct railway connections with London, Cambridge and Oxford, letting scientists and the army forces to travel with a low profile.

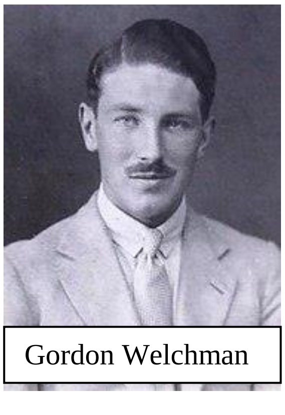
Some of the first people to arrive at Bletchley Park were professional codebreakers, mathematicians and even chess players or people with excellent organising skills, known as 'bombes'. Among them are Alfred Dillwyn Knox, the former codebreaker in World War One, Gordon Welchman and Alan Turing who were both top class mathematicians that studied at Cambridge, and Stuart Milner-Barry who was a professional chess player and writer.



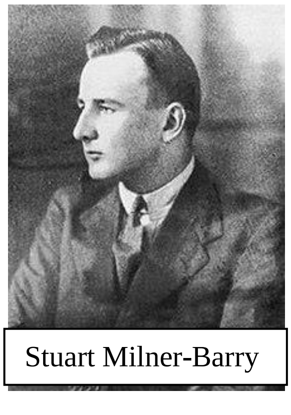
Alfred Dillwyn Knox



Alan Turing



Gordon Welchman



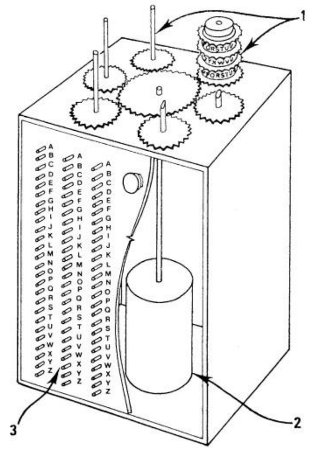
Stuart Milner-Barry

Chapter Four: The British Bombe

Based on the information introduced by the Polish Cipher Bureau, British mathematicians Alan Turing and Gordon Welchman, soon after, develop a machine capable of recovering the key settings of the Enigma, even if the Germans would drop the double encryption of the message key at the beginning of any message. The machine was called the Bombe, (later called the Turing-Welchman Bombe) and would become crucial to the Allies when discovering the Germans' next moves.

The name Bombe was derived from 'Bomba', the name of a similar machine developed by the Poles before the outbreak of World War Two. The Polish Bomba capitalised on the fact that the same message indicator was sent twice at the start of every single message, which was a major flaw in the German cryptographic procedures. Turing wanted to try a different approach to cracking Enigma, as the concept of the Bomba was already known to Bletchley Park. The Germans eventually discovered the flaw in their double encipherment of message indicators that they gave up on it on most radio networks, making the Bomba useless.

Turing, with help from Welchman, designed the British Bombe in 1939. Compared to its Polish counterpart, they used a completely different approach. It was based on their assumption that a known or unknown plaintext or a 'crib' is present at a certain point of any message about to be sent. The British Tabulating Company at Letchworth in the UK built the first Bombes. The first machine, called 'Victory', was delivered at Bletchley Park on the 18th March 1940.



8. Bomba kryptologiczna

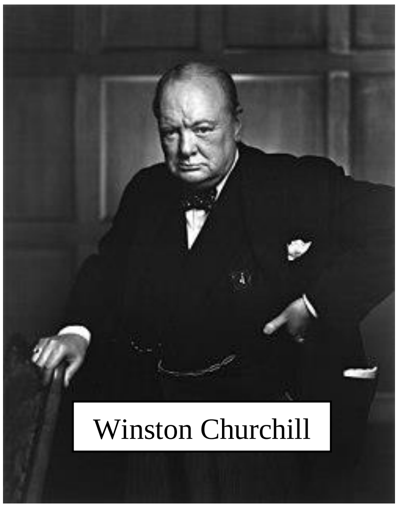
(dla przejrzystości ukazano w górnej części bomby tylko jeden zestaw wirników szyfrujących)

1. wirniki,
2. silnik elektryczny,
3. przełączniki

A diagonal board further enhanced the Bombe to reduce the number of steps needed for the codebreaking effort. A second Bombe, featuring Welchman's diagonal board, was installed on the 8th August 1940. It was named 'Agnus Dei' and motivated 'Victory' to be modified with a diagonal board as well.

During the course of World War Two, over 200 Turing-Welchman Bombes were built. They were spread across Bletchley Park and its 'outstations' in Wavendon, Adstock, Gayhurst, Eastcote and Stanmore, and ran by technicians and civilian personnel to prevent the risk of losing any of the the machines to a bomb attack. The Bombes took long to perfect but, in my opinion, helped win World War Two for the Allied forces.

Chapter Five: Top Secret Ultra


Winston Churchill

Winston Churchill became the Prime Minister after Neville Chamberlain resigned on the 10th May 1940. He completely recognised the utility, impact and importance of the intelligence discovered by Bletchley Park and the Bombe during World War Two. He introduces a new level of confidentiality that exceeds all other levels, he called it Top Secret Ultra, abbreviated to ULTRA, and states that the source of this ULTRA intelligence had to be kept classified with no exceptions.

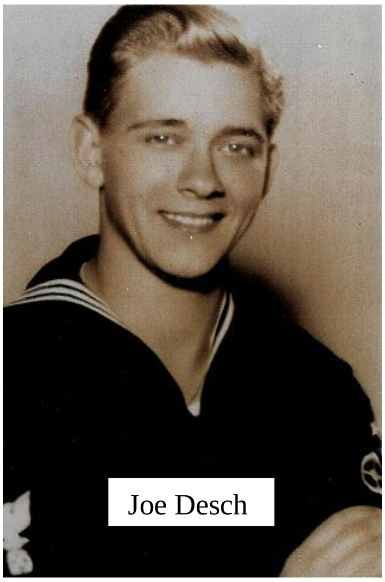
By 1940, British codebreakers were able to read massive amounts of Germany's radio messages from the German Luftwaffe and a fair amount of the Wehrmacht's traffic. On the other hand, the Kriegsmarine's messages had more complicated operating procedures, and furthermore, had three additional rotors, which posed as a real problem as the wiring of these rotors was unknown. The three additional rotors were exclusive to the German Navy and were not used in any other division of the Army.

In 1941, Alan Turing discovered the wiring of the additional wheels and the naval intelligence indicator procedure. Aided by the catch of a large amount of codebook that was captured on the 9th May 1941, Turing had managed to find a way into the Naval Enigma and decrypt part of the naval traffic. He figures out that the Kriegsmarine used a complex strategy that involves numerous amounts of codebooks, short message books and substitution tables. The long messages and status reports that were discovered are shortened by translating them into a short letter combination.

Suddenly, on the 2nd February 1942, the German Kreigsmarine introduces a new Enigma machine out of nowhere, which causes an extreme blackout for the codebreakers at Bletchley Park.

The new Enigma machine had an extra cipher wheel that was installed between one of the furthest left wheels and the reflector. At the same time, the indicator system was changed and new codebooks were introduced. The new machine was known as the Enigma M4 and is used exclusively by the U-Boot section of the Kriegsmarine. The Turing-Welchman Bombes that were made for the 3-wheel Enigma were not suitable for the new Enigma M4, which made the codebreakers at Bletchley Park start from scratch.

Chapter Six: The American Bombe


Joe Desch

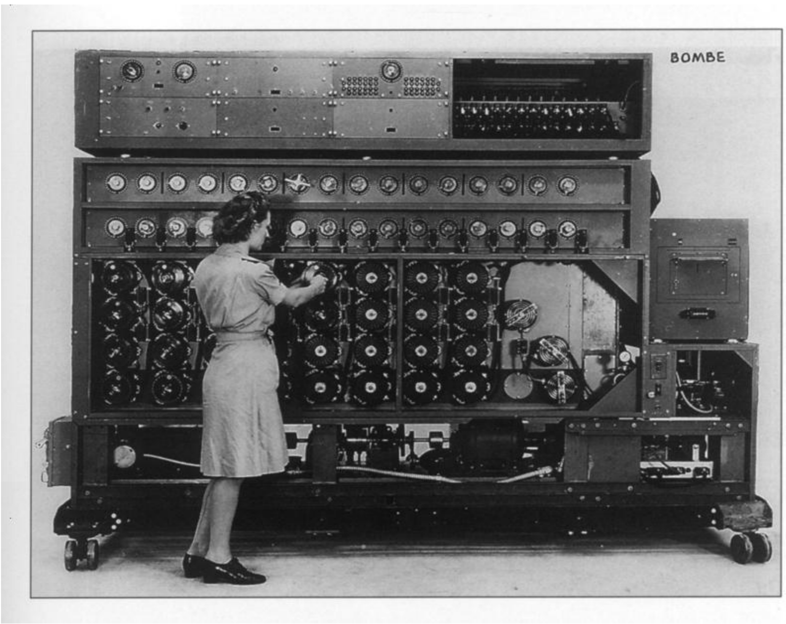
Although the British Bombe worked to its expectations, it faced many problems along the way. At this stage of World War Two, Britain had shortages of almost everything. The Bombe machines were not delivered on time and the machines that got to their destination often had communication problems.

Since the Americans were strongly involved in 1942, they kept on pushing the British to share their knowledge about the Bombe and allow them to recreate its design. Finally, in late 1942, with the British Bombe was facing problems and the casualties at the Battle of the Atlantic were growing, the British finally allowed the Americans to build their own Bombe.

The 'US-Bombe' was built by the National Cash Registers in Dayton, USA, where it was developed by a man called Joe Desch. The US Navy had previously wanted him to build an electronic Enigma, but Desch proved it to be impractical, as the machine would need more than 70,000 electronic valves in a minor limit. Towards the end of 1942, Desch proposed a less elegant and advanced but a more realistic approach; an electro-mechanical machine, which was just like the British Bombe, but was more reliable and faster. The US Navy, impressed with Desch's machine, immediately approved of the project.

Desch had set out to build the machine and by mid-1943, he got his first prototypes running. Even though the first design encountered some reliability problems, Desch managed to improve it. By December 1943, 120 machines were installed all around the country. With the help of the US-Bombe, America took care of cracking the majority of German Naval Enigma traffic, especially the messages from the German U-Boats.

Desch's US-Bombe, not to be confused with the British Bombe



Chapter Seven: The Aftermath

Germany surrendered on the 7th May 1945, bringing an end to the 6-year war and the Bombe. All British bombes were destroyed or dismantled after the war was over and so was its history for a few decades. People went on with their lives and there wasn't much traces left of any of the Bombe machines created.

People had continued to use the Enigma-I machines long after World War Two; Norway, Germany and Austria, until they were replaced for newer and better equipment.

The Turing-Welchman Bombe is said to have been vital to the win over the Axis powers, it may have shortened the war by at least 2 years and saved 14 million lives. In my point of view, the Bombe had gotten the Allies back into a winning position, they had started to run out of supplies and soldiers and the Bombe had prevented the war being longer, so they didn't need to use up all they had.

The Enigma had encouraged countries to make their own cipher machines, in 1956, the Russians introduced the first model of their advanced rotor-based cipher machine named FIALKA. The machine had 10 different cipher wheels and featured irregular wheel stepping, with the wheels moving in both directions to make the code more difficult to crack. More importantly, they had found solutions for all of the Enigma's weaknesses, for example, a letter can never be encoded into itself.

Additionally, the 'Steckerbrett' was replaced with a card reader, the machine operated directly on tele printer signals, enabling the use of letters and numbers. It also had a built-in tape puncher and reader, and printed the output directly onto a paper strip. It became officially known as the M-125 and was used by all the countries involved in the Warsaw Pact.

Chapter Eight: British Intelligence in WWII

It is arguable that technology played a greater role in the conduct of World War Two than any other war known in history, and had a critical role in its final income; it was the first war where military operations targeted enemy research efforts. The Allies had started to pay a lot of attention to military operations and intelligence gathering straight after World War One up to the imminence of World War Two.

They had two major security services operating at the time for that, MI5 and MI6, who would often work with British Intelligence to steal the ideas of airborne operations, synchropters (or intermeshing rotors), jet-powered aircraft, cruise missiles, methamphetamines and rockets from the Axis powers. The Allies often co-operated on the development, manufacturing of new and existing technologies to support military operations and intelligence gathering.

Not only did Britain steal game-changing plans from the Germans, but they also intercepted German communications and fed misinformation back to Germany. They had a great success in uncovering enemy agents in Britain, and turning them into "double agents", agents from the Axis powers that would feed information to the British from their job in German Intelligence, and feed wrong information back to the Germans after their trip to Britain. The Double Cross system helped the Allies immensely; it became a highly effective deception and led to many more double agents joining soon after. The Joint Intelligence Committee, started by seven individuals, had provided intel input from "Operation Torch" and turned it into a large, strategically important military offensive.

Intelligence at the time did not only mean espionage, it meant aerial reconnaissance, or aerial photography, which was used as a key method into obtaining information about their enemy, as photographs were concrete evidence fast, after three stages, often completed in an hour. Allied reconnaissance involved mapping and damage assessment, where enemy activity was recorded so that accurate maps, for the ground army, could be made. From damage assessment photographs, the exact moment when a target should be re-attacked after a previous hit, could be calculated, and the effectiveness of the enemy's recovery programme could be analysed. Radars, equipment developed before the war, were powered by radio waves and were used to detect enemy aircraft that were attempting to attack unsuspectedly with the help of sonar sound waves, which were used to identify distant objects, like the Axis' fighter planes and submarines.

Yet, Germany were still at the forefront of industrial warfare at the time, producing the first jet-powered bomber, the first tilt-rotor plane and fission, and when the Allies found out about their growing war industry. They had a hard time closing technological gaps from German advances, but Britain's strong intelligence forces controversially gave the Allies an extra edge over the Axis' technology.

Chapter Nine: German Intelligence in WWII

On the other hand, the Germans had their fair amount of intelligence but it was debatable to be much worse than the Allied forces. Compared to the successes achieved by the Allies, with the cracking of the Enigma code, the successes from German intelligence were not as outstanding but were accomplishments nonetheless.

Like the Allies, the Germans' greatest successes came from the field of communications intelligence. Germany set up listening posts in Spain and traded cipher information with the rest of the Axis powers. The Allies are famously known for their code breaking with the Enigma and the Bombe, but even though they are not well known for it, Germany did not ignore code breaking. The Germans broke the ciphers of every Allied nation except Stalin's Soviet Union.

World War II Allied/Axis
Individual countries
Green- Allies before the attack on Pearl Harbor
Blue- Allies after the attack on Pearl Harbor
Black- Axis Powers
Red- Russia started Axis and switched to Allied
Gray- Neutral or not involved countries

German Lieutenant General Erwin Rommel's best source in North Africa was the American military attaché in Cairo. Rommel "regularly read" his detailed reports on British forces, because of German code breaking. Code breaking also enabled the German Kriegsmarine to know the positions of the British Navy before Germany's invasion of Norway in 1940.

Germany also had the ability to intercept high-level communications. A German radio intelligence post in the Netherlands supervised and managed to crack the radiotelephone conversations between Franklin D. Roosevelt and Winston Churchill in real time. The exchanges were recorded and translated for Adolf Hitler, but the effort had provided very little intelligence. Similar times when the Germans used communications eavesdropping, gave Hitler intelligence on Czech Republic's intentions in 1938 and those of Britain, France, and Poland a year later.

Even intercepting text messages and radio communications led to German intelligence successes. The Germans already intercepted messages and tapped phones in Germany to avoid anti-Nazi propaganda. They prided themselves in managing to exploit intercepted communications for commanders so that it was actionable intelligence.

Surprisingly, most German spies mostly failed, even though they were very good at infiltration of intelligence, but a few did succeed. One of the spies passed along the blueprints to the Norden bombsight in 1937. The Germans then reconstructed a copy and made improvements to their own sights based on Norden. Another spy visited many American war factories, thanks to his deep cover and fast-talking. Germany managed to infiltrate some spies into New York City, although those agents were not efficient or useful. The deadly mission involved a U-boat dropping off the agents in Maine on a snowy night, but when they got to New York, the spies quickly forgot their mission and failed it, which, in my opinion helped the Allies gain the intelligence edge over the Axis powers, since they were much more prepared for missions.

Pros and Cons of the Bombe

PROS	CONS
The Bombe had been so essential to the war effort of the Allies, its estimated to had shortened the war by 2 years and save 14 million people from death.	Its building process took around 4 years, the Bombe was only just fully developed in the middle – near end of World War Two, it took too long to make more machines and get them delivered to different places.

Conclusion

In conclusion, the Allies cracking the Enigma code did define their victory as, in my opinion; it helped them out immensely when they wanted to be one-step ahead of the Axis powers. As said in Chapter Seven, people have estimated that the war would've gone on for at least 2 more years and 14 million people would have died without the Bombe being created. With the Allies running short of supplies and soldiers, the Bombe had been proven to be much more useful than its original purpose, cracking a code, it helped save many more lives that would have been taken away.

But not to forget, the Bombe still helped the Allies by cracking the Enigma code, the Enigma was dangerous, the Germans had spent a decade or more trying to perfect one piece of equipment, it must have been that important to them. No one would spend that long trying to improve something that had not even been in proper use yet. This comes to show how crucial the Enigma machines and prototypes were for the Axis powers. They thought that something they discovered, something that they had improved for so long, could make something so difficult that it could be literally impossible to crack, which is why they panicked and kept on developing the Enigma, especially when they found out Bletchley Park had intercepted most of their important messages. They believed that if they kept making it harder on the British and themselves, that the cryptanalysts in the Allied countries would eventually give up on trying cracking Enigma.

There were also plenty of different factors that contributed to the successes of the Allies, in my opinion they were more advanced and intelligent, they were smart enough to try and take important projects and information from their opponents and turn it into their own. The soldiers and sailors held it out even though they watched their men drop. Even when the Germans technologically and tactically outsmarted them, they used everything they had left to win the war; certainly, the world would have been different if the Allies were defeated.

Bibliography

Websites

http://www.cryptomuseum.com/crypto/enigma/hist.htm

http://www.bbc.co.uk/history/topics/enigma

http://armchairgeneral.com/german-intelligence-successes-in-world-war-ii.htm

http://www.bbc.co.uk/history/worldwars/wwtwo/aerial_recon_gallery.shtml

https://www.tandfonline.com/doi/abs/10.1080/0161-119091864733 (extract of the book by F.H Hinsley)

http://www.cryptomuseum.com/crypto/bombe/

http://www.bbc.co.uk/history/worldwars/wwtwo/mi5_ww2_01.shtml

https://www.bletchleyparkresearch.co.uk/research-notes/how-successful-were-hitlers-codebreakers/

Books

British Intelligence – In The Second World War Vol.1 by F.H Hinsley, Her Majesty’s Stationery Office, 1979

Spying On the World by J. Aldrich, 2014

In the Name of Intelligence, in Honor of Walter Pforzheimer, NIBC Press