Isaac Cardello

Mrs. Awde

AOIT 1

22 May 2020

Enigma Machine: The Fate of World War 2 and Millions of Lives

Throughout World War 2, information was vital to plan and attack against an enemy. Due to this vital need of information, the field of cryptology boomed. A new type of war broke out, not between soldiers, but between code makers and code breakers. Countries like Germany had major involvement in World War 2, thus leading forces like the German army needing a way to send information without letting the enemy know what the code really meant. This led to the invention/discovery of the enigma machine, a German cryptographic machine to cipher and decipher messages with trillions of possibilities. The enigma machine played a major role in the war as it may have totally changed the fate of the war but most definitely affected the lives of millions of people each day with the secrets encoded in each German message.

To understand the importance of the enigma machine, a brief history of the enigma machine and Germany during World War 2 is needed. The enigma machine was not created in one particular place in one particular moment, but was created throughout the duration of 1917 by Edward Hebern in America, Arvid Damm in Sweden, Hugo Koch in The Netherlands and Arthur Scherbius in Germany (History of the Enigma). The official creator of the enigma machine has been given to German electrical engineer Arthur Scherbius, who created the enigma machine around the end of World War 1. He released his first commercial enigma machine to the public in 1923 and from then on, the enigma machine went through 14 more stages until finally becoming the Railway. Not jumping ahead, the first enigma machine was titled “Enigma A” and

was quickly replaced by “Enigma B”, an improved enigma machine. Some of the improvements were things such as an improved printing wheel. This process of selling and improving the enigma went on until 1932 when the German army claims all ownership of the machine.

Moving onto the history the battle of code makers and code breakers of World War 2 will help to explain why the enigma machine and ultimately finding a way to break the enigma cipher was so important during World War 2. The enigma machine was commercially open to the public until 1932 when the German army seizes complete ownership of the machine so all sales of the enigma machine must be approved by the German army. The German army starts selling enigma machines like the model H to the Hungarian, Swiss, and Dutch army. In 1930, the polish is very worried of an attack from Germany as they are on the border of Germany. The polish is the first to try and crack the enigma machine cipher. The polish government hires 3 young but brilliant mathematicians to crack the enigma machine cipher. The mathematicians hired by the polish government were Marian Rejewski, Jerzy Rózycki and Henryk Zygalski (History of the Enigma). To crack the enigma cipher, all they are given is a bunch of intercepted messages encoded in the enigma cipher and a description of the commercial model enigma machine. In late 1932, Rejewski figured out the internal wiring of the enigma machine. This is the first breakthrough the trio figured out and many more were soon to come such as the exploitation of a double ciphered message. Other ways of gaining information about the enigma machine also leaked from Germany such as a German playboy working at the German Cipher Office selling information to the French for money in 1933. This allowed the French to sell the information to the Polish and let the Polish build an enigma machine of their own. The final nail in the coffin to crack the enigma cipher was Alan Turing and his invention of the Bombe machine. On August 14, 1939, Bletchley is built in the United Kingdom to break ciphers and codes. The first people

to arrive at Bletchley were mathematicians, code breakers, and master chess players such as Stuart Milner-Barry, Gordon Welchman, and Alan Turing. Alan Turing, a mathematician from Cambridge soon builds a machine that can crack almost any message enciphered by an enigma machine in under 20 minutes. He did this by taking a different approach to breaking the enigma cipher, he would assume a certain word in a message meant a certain German word based off of its position (citation). Based off of this assumption, the machine would start guessing the words of other enciphered words based off of their position as well.

The cracking of the enigma machine is extremely important as it enabled countries like Britain and France to plan around the attacks of the Germans. One example of this is planning around the German U-Boat attacks. Bletchley was flooded with German messages about the location and directions of the U-Boats in the Atlantic Sea. The German U-Boats were submarines made to sink carriers travelling from America to Britain while sailing the sea. With the Alan Turing's Bombe machine cracking these encrypted messages within minutes, the carriers could avoid the locations of the German U-Boats and safely travel from each destination. This not only had a huge impact on the war as Britain and allies of Britain were getting their supplies regularly from the carriers since they avoided the U-Boats, but saves hundreds of thousands of lives (J. Copeland). When German U-Boats sank the carriers with their torpedoes, the Germans would take any remaining sailors that made it out of the ship alive back to prison. This saved the lives of many sailors working aboard the carriers. By detouring around the U-Boats, the war also may have been shortened as attacks like D-Day could have been delayed since combat ships had to travel over the Atlantic to reach Britain and attack Germany. The delay of the D-Day attack could have led the war to continue for two to three more years and kill an estimated 14 to 21 million more militants (J. Copeland).

For Alan Turing to crack the enigma machine, he needed to figure out how the machine worked but more importantly, the major flaw of the enigma machine. The enigma machine works by the user pressing a letter on a keyboard like one of a type writer. The keyboard sends an electrical signal through a device called a plug board. The plug board had 26 slots on it with holds to plug electrical wires into. With the plug board, the electrical wire hooked up to the letter, “k” for example, could be plugged into the slot for “q” This was only the beginning or else the enigma machine would have been stupidly easy to solve as there is a very small number of combinations to run through. Once each electrical wire was plugged into different slots, the electricity ran through 3 rotors inside of the machine. Each rotor had 26 sides to it and each side represented a letter. Inside the rotor, wires were hooked up to different ends of the sides. For example, the letter “a” at one side of the rotor came out as “h” on the other side of the rotor. The electricity would run through 3 different rotors which raised the number of combinations to the millions but the machine is not nearly done. Once the electricity traveled through the plug board and 3 rotors, it traveled into a reflector which sent the electrical signal back through the 3 rotors in a different path. This sent the amount of possible combinations into the billions as the electricity then ran into one of 26 wires based on the output of the rotor it came out of. The wire it came out of was hooked up to a light bulb with a letter printed on top of it. After this, the first rotor would turn 1 interval and create a new path for the electricity which ultimately made the electricity light up a different bulb. This would repeat for each rotor until each rotor got to its 26^{th} side and would then start to move the next rotor by 1 interval. This process was so hard to crack since the same letter could be pressed multiple times and always come out as something different due to the fact the rotors would turn and create a new path (Hern).

This method of encryption was almost perfect at the time if the Germans had not made 1 fatal mistake. The fatal mistake was the fact a letter could never be output as itself. The letter “a” could never come out as “a” and this was true for any other letter as well (Hern). This was because the reflector would never send the letter the same way it came in. Alan Turing used this to his advantage as the number of rotor combinations was drastically reduced due to this flaw. This heled the Bombe do much faster computational work. Without this flaw, it would have taken the Bombe many years to decipher one message if it was not programed with the recognition that no letter could be itself. Add to the fact that Alan Turing used commonly used phrases to guess parts of the German message as the Germans never switched the format of their messages and you have a encoded message that can be broken in under 20 minutes. Mathematicians cracking codes on paper, the Bombe and other variations of the machine running through hundreds of thousands of rotor combinations per day, and exploiting the flaws of the enigma machine is what ultimately cracked the code.

Moving on from the history of World War 2, the enigma machine is still important today. Some modern contributions to the importance of the enigma machine are the movie *The Imitation Game* and Quantum Enigma, a branch of quantum mechanics. The reason the enigma machine is getting the attention it deserves is because the British could not tell anyone they cracked the enigma machine cipher or else the Germans would have created a whole new cipher which would have prolonged the war. Alan Turing died with the secret that saved millions of lives and has only recently been getting the well-deserved attention for the importance of the Bombe and the enigma machine. To put a very long and complex time line into one sentence, the enigma machine may not have affected the war directly but secretly impacted the lives of millions and impacted some small parts of the war to possibly have huge consequences.

Works Cited

Copeland, B. Jack. *Colossus: Its Origins and Originators*. Canterbury: IEEE Annals of the History of Computing, 26(4), 38-45., 2004.

Copeland, Jack. *Alan Turing: The codebreaker who saved 'millions of lives'*. 19 June 2012. Document. 7 June 2018.

Hern, Alex. *How did the Enigma machine work?* 14 November 2014. Document. 7 June 2018.

History of the Enigma. 14 March 2012. Document. 30 May 2018.