5-2015

All the King's Men: British Codebreaking Operations: 1938-43

Andrew J. Avery
East Tennessee State University

All the King's Men:

British Codebreaking Operations: 1938-43

A thesis

presented to

the faculty of the Department of History

East Tennessee State University

In partial fulfillment

of the requirements for the degree

Master of Arts in History

---

by

Andrew J. Avery

May 2015

Dr. Stephen G. Fritz, Chair

Dr. Andrew L. Slap

Dr. John Rankin

Keywords: World War II, Alan Turing, Bletchley Park, Code-breaking, Room 40, Gordon Welchman, GC&CS

ABSTRACT

All the King's Men:

British Codebreaking Operations: 1938-43

by

Andrew J. Avery

The Enigma code was one of the most dangerous and effective weapons the Germans wielded at the outbreak of the Second World War. The Enigma machine was capable of encrypting radio messages that seemed virtually unbreakable. In fact, there were 158,900, 000,000,000 possible combinations in any given message transmitted. On the eve of the war's outbreak, the British had recently learned that the Poles had made significant progress against this intimidating cipher in the early 1930s. Incensed and with little help, the British Government Code & Cipher School began the war searching for a solution. Drawing from their experiences from the First World War, and under the visionary guidance of Alan Turing, Gordon Welchman, and countless others, the British created a new, mechanical approach to breaking the seemingly impossible German code. By breaking the code, they could very well save Britain.

ACKNOWLEDGEMENTS

I would like to begin this thesis by thanking just a few of the people who helped me during this process. First and foremost, I would like to thank Dr. Stephen G. Fritz, who has guided me from the very beginning of this project, offering not only feedback, but encouragement from the conception of the topic to its completion. Dr. Fritz was my first point of contact at East Tennessee State University, and was one of the deciding factors in my choosing to undertake my Master's degree at this institution. Dr. Andrew L. Slap, whom I had the pleasure of working for as a Graduate Assistant for two semesters, has also given me plenty of advice about all things pertaining to the academic field and served as a point of reassurance. Dr. John Rankin supplied me with essential information about researching at the National Archives, staying in Kew, and researching in the United Kingdom. Without his help, my primary source research would not have gone as smoothly as it did. Countless other faculty members at East Tennessee State have proved helpful: Dr. Doug Burgess and Dr. Daryl Carter shaped the foundation of my graduate education. Dr. Philip K. Wilson, Department Chair, has also proved to be full of advice and good humor when it has been most needed. Sharon Chandler, the staff of the Sherrod Library, and the graduate student community have all been extremely supportive helpful over the past two years.

I would also like to think the staff of the National Archives at Kew, the British Library, and Richard Lewis, the archivist at the Bletchley Park National Trust. My historical education was enriched by four professors at my undergraduate alma mater, Flagler College, and they deserve notice. Without Dr. J. Michael Butler, Dr. Wayne Riggs, Professor Steve Voguit, and Dr. John Young, I would not have written this thesis, or decided to pursue a graduate degree. Finally, I would like to thank my family and close friends for their love and support over the years.

CONTENTS

CHAPTER 1

INTRODUCTION

The White Rabbit put on his spectacles. “Where shall I begin, please your majesty?” he asked.

“Begin at the beginning,” the King said, very gravely, “and go on till you come to the end: then stop.”

--Lewis Carroll, *Alice’s Adventures in Wonderland*

On the morning of 8 June 1954 Alan M. Turing was found dead in his lodgings in Wimslow, Cheshire.[1] He had committed suicide by infusing cyanide into an apple and eating it. At the time of his death Turing had been working on developing computer technology at the University of Manchester. In the days following Turing’s death there were many dedications and reflections written about him. “In the death of Alan Turing,” wrote one author “mathematics and science have lost a great original thinker.”[2] Turing was described as an “even-tempered, lovable character with an impish sense of humor” in *The Shirburnian*, the publication produced by Sherborne, Turing’s public school alma matter.[3] In all the accounts written about Turing there was little mention of his war time work, only that it was “hush-hush” and that he had been awarded an O.B.E for it.[4] Except for these brief comments, there was nothing to be said about how Turing had spent five and a half years of his short, productive life. From these scant clues one could only deduce that Turing’s wartime work was of vital importance. Knighthoods were not given to just anyone.

[1] The Turing Digital Archive, *About Alan Turing*, *http://www.turingarchive.org/about/*, *(*accessed 18 January 2015.)

[2] The Turing Digital Archive, “Dr. Alan Turing: An Appreciation,” published in the *Manchester Guardian*, 11 June 1954, http://www.turingarchive.org/viewer/?id=452&title=10b (accessed 19 January 2015)

[3] The Turing Digital Archive, “A.M. Turing, (h.1926-31)” published in *The Shirburnian*, Summer Term 1954, http://www.turingarchive.org/viewer/?id=452&title=6 (accessed 19 January 2015).

[4] *Ibid.*

Turing was not the only person whose wartime service remained shrouded in intrigue in the years following 1945. There existed within Britain hundreds of men and women who had signed the Official Secrets of Act and therefore had forfeited the right to share six years of pivotal personal history. In a generation when wartime service was a crucial part of identity, a whole sub-group remained silent. Only a few people knew that Turing, along with dozens of other brilliant people, had spent the entirety of the Second World War feverishly battling one of the greatest German threats of the war: the Enigma code.

The British struggle to break the Enigma code lasted from 1939-43. It spanned multiple theatres of combat, and across thousands of miles of land, sea, and air. There were no front lines. The battle was fought every day over the airwaves and in the facilities at Bletchley Park. Early in the war, after Britain had been chased off of continental Europe, the pressure on the codebreakers was ratcheted up further. Even after the immediate threat of a German invasion of Britain subsided, an aggressive U-boat campaign in the Atlantic kept the men and women of Bletchley Park working feverishly every day to ease the strategic strain on Britain.

The deeds of the codebreakers remained a state secret for nearly thirty years following the war. The long-kept secret was broken in 1974 when F.W. Winterbotham published his first-hand account of his work at Bletchley Park.[5] *The Ultra Secret* was the first English language account of British codebreaking during the war. The public had been exposed to British codebreaking exploits of the First World War in Barbara Tuchman's *The Zimmermann Telegram*

[5] Winterbotham's book constituted a violation of the Official Secrets Act of 1911. He did not, however, face prosecution from the British Government. A cursory glance at the historical record reveals that Winterbotham was not the first former British codebreaker to reveal his trade secrets to the public. Ten years following the First World War, Alfred Ewing delivered a public lecture about his wartime work in Room 40. This incident will be described and analyzed later in this thesis. It seems that both Ewing and Winterbotham were able to escape prosecution by being selective with the details they provided. Even though they revealed state secrets, apparently their conscience did not allow them to reveal technical and more incendiary secrets.

only sixteen years earlier. Winterbotham's *The Ultra Secret* shed light on yet another chapter of British cryptological history. The British had done it yet again, it seemed, broken a code that saved Britain. Winterbotham's account of the events at Bletchley Park extended a beloved stereotype: British amateurs bumbling their way through things and saving their country and possibly the world, along the way. If only they had done it alone.

Unlike Tuchman's *The Zimmermann Telegram, The Ultra Secret* did not award codebreaking credit solely to the British. Winterbotham briefly mentioned the pre-war efforts of a group of Polish codebreakers. According to him, these Poles had contributed to, and broke the Enigma code before the British. Eight years following the publication of *The Ultra Secret,* Peter Calvocoressi, who had overseen the Air Section of Bletchley Park, published his own account of British codebreaking: *Top Secret Ultra.* Calvocoressi also mentioned the Poles in his work, but much like Winterbotham, he only mentioned them in passing. Gordon Welchman, who had helped design codebreaking technology with Turing, wrote *The Hut Six Story* the same year as *Top Secret Ultra* was published. Welchman's account differed slightly because Winterbotham had not been directly involved in codebreaking, but instead with the counterintelligence effort to prevent the Germans from discovering the British break. Welchman had been on the ground floor of breaking Enigma from the beginning, whereas Winterbotham had been working in an entirely different department. Welchman mentioned the Poles also, but like the previous two authors he brushed past them. From these three works one's viewpoint of how the Enigma was broken was lopsided in favor the British. The Poles had contributed, but how much and in what way?

The year following the publication of Welchman and Calvocoressi's books, Wladyslaw Kozaczuk's *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by* *the Allies in World War Two* shattered the historiographical gridlock. Aided greatly by appendices written by two of the Polish codebreakers, Kozaczuck's work turned the historic record on its head. Kozaczuck placed a high premium on the pre-war work of the Poles. He contended that Polish advances were intrinsic to the breakthroughs later accomplished by the British. This opinion was also strongly echoed by Hugh Sebag-Montefiore's *Enigma: The Battle for the Code* published in 2000. There have been dozens of other books written about the Enigma code, and the various authors' take on the Polish contribution splits down the middle. In any worthwhile account of the code, one must, at the very least, mention the pre-war work of the Poles. Authors have struggled to decide which is more important: who broke the code first or who broke it at the most opportune time? How valuable were the Polish contributions to later British efforts? In short, could the British have broken the code without the Poles?

In short, yes. The British could, and they did. The Polish contributions practically occurred in a vacuum. The British had to rely on their own methods to crack the code.

I contend that while the Poles were able to make significant strides against the early versions of the Enigma code and develop the preliminary technologies to make the breaking of the code feasible, their prolonged silence on the subject made their contributions practically null and void. By the time the Poles had shared their outdated progress with the British and French in August 1939, it was too late. The silence of the Poles resulted in the British refusing to seriously collaborate with any of their allies. The British were able not only to develop similar methods for breaking the code, but improve upon those methods substantially with minimal assistance from the Poles or their methods.

This thesis will analyze the efforts of both the Polish and British codebreakers as each nation confronted the seemingly unbreakable German code. Firstly, it is important to understand the growth of British intelligence and codebreaking, branches of the government that emerged permanently due in part to invasion paranoia of the Edwardian era and the First World War. Many of the practices of British codebreaking, specifically in recruiting personnel, were established from 1914-18. It was because of their wartime work that British codebreaking was able to survive during the interwar period. Secondly, I will trace the creation and development of the Enigma machine and code by Arthur Scheribus, and its adoption by the German military during the 1920s.

In the second chapter I will also elaborate on the analytical response of the Polish Cipher Bureau. The Polish Cipher Bureau managed to break and earlier, simpler version of the Enigma code, and monitor encrypted German radio traffic for a short period of time. It was their failure and frustration, as well as mounting German militaristic aggression that led the Poles to share their progress with the Allies.

Finally, I will discuss the British response to the code and how their efforts differed and yet were similar to those of the Poles. In short, the British were able to take some of the methods and technologies pioneered by the Poles and improve upon them significantly. The British were able to crack the code more efficiently. I will explain how the staff at Bletchley Park devised the technology and the methods that allowed them to consistently break the Enigma code.

Even though this thesis focuses on the codebreaking efforts of both the British and the Poles, my perspective stems from and is directly concerned with British perception. This is due, in part, to the general lack of primary sources available from the Polish Cipher Bureau. It seems that none of them survived the war.

The British and Polish battle against the code was not waged on the front lines, or with conventional weapons. Instead, the battle was fought every day using radio waves, early computers, pencil, paper, and the human mind. The struggle against the code would last, in sum total, from 1927-43. The Enigma code, and the saga of those who struggled to break it, is an important aspect of the Second World War, and the breaking of the code quickly became an intrinsic chapter in the British saga of the war.

CHAPTER 2

THE GENESIS OF BRITISH INTELLIGENCE & CODEBREAKING, 1905-19

"To be weak is to invite war: to be strong is to prevent it."

—William LeQueux, *The Invasion*

In the article "Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects," David Kahn writes that "between the Metaurus and the twentieth century signal intelligence did not help armies win any more major battles."[6] Intelligence gathering and the wide use of encrypted messages in warfare did not proliferate until the twentieth century. Although intelligence had played a role in conflicts before the twentieth century, signals intelligence became an integral part of how modern armies and nations fought conflicts. The way in which wars are fought constantly change with the development of new technologies. Radio technology revolutionized warfare and intelligence. Like many nations at the beginning of World War I, Great Britain's intelligence community was relatively young. In order to understand the origins British codebreaking and how it reached optimal operating levels at Bletchley Park during World War II, it is vital to understand the formation, development, and establishment of the British intelligence community as a whole. British codebreaking and British intelligence share the same genesis, born in part of invasion paranoia and the First World War.

This chapter will trace the three key elements that led to the establishment and professionalization of the British intelligence community and codebreaking operations: the establishment of the Secret Service Bureau, the passage of the Official Secrets Act of 1911, and

[6] David Khan, "Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects," in *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*. Edited by Christopher Andrew & David Dilks. (Urbana & Chicago: University of Illinois Press, 1984).

the outbreak of World War I. In addition to these three factors, I will also explore the influence that Winston Churchill had on the early foundations of the British intelligence community, and the importance of social class on the recruitment of intelligence officials.

The British have long taken part in what Christopher Andrew dubbed "the world's oldest profession."[7] Intelligence gathering and spying have been a vital part of the British government since the reign of the Tudors.[8] Institutions such as the Foreign Office served as a precursor to the foundation of official intelligence organizations; that is to say the creation of an organization that specialized exclusively in the gathering, analysis, and distribution of intelligence on domestic and international fronts. It was not until October 1909 that the British government established the British Secret Service Bureau, the predecessor of both MI5 and MI6.[9] According to Rhodri Jeffrey-Jones there were several factors that led to the establishment of the Secret Service Bureau. The first of which was competition. The German admiralty staff had established its own intelligence branch in 1901. The British and Germans had been engaged in an aggressive naval and militaristic build-up spurred on by nationalistic and imperialistic motives. It was only natural that the British would establish their own intelligence departments in order to maintain the status quo.[10] In addition to competing with the Germans, Jeffrey-Jones contends that "journalists, novelists, and politicians fanned fears of invasion, and promulgated the views that a German spy network was putting British defenses in peril."[11] There was a very authentic sense of paranoia

[7] Christopher Andrew, *Her Majesty's Secret Service: The Making of the British Intelligence Community*, (New York: Penguin, 1985), 2.

[8] Andrew, *Her Majesty's Secret Service*, 2.

[9] Rhodri Jeffrey-Jones, *In Spies We Trust: The Story of Western Intelligence,* (Oxford: Oxford University Press, 2013), 12-13.

[10] Jeffrey-Jones, *In Spies We Trust,* 12-13. The traditional origin myths of World War I have come under some considerable—and well deserved—scrutiny some ninety years after the fact. Christopher Clark's *The Sleepwalkers: How Europe Went to War in 1914* has offered some new glances into the motives behind the outbreak of the conflict. However, it is not necessary to delve into a historiographical debate in this particular worth.

[11] Jeffrey-Jones, *In Spies We Trust,* 13.

throughout Edwardian Britain, and the government was just as worried as the populace they governed.

Prior to the establishment of the Secret Service Bureau, the Germans were not the only catalysts spurring on the development of a formal intelligence organization in Britain. The rising sense of Irish nationalism and the Boer War caused significant concern in the British government and led to short-lived attempts at creating intelligence gathering organizations. As early as March 1883 Scotland Yard had established the “Special Irish Branch” in Dublin in order to intercept possible bomb plots against the British government.[12] An initial bomb plot in early 1881 had left a seven year old boy dead, and there were fears that the attacks may escalate and possibly be used to harm members of the royal family.[13] The Special Irish Branch did not prove successful. Despite cooperation with the Royal Irish Constabulary and some minimal successes the Special Irish Branch was eventually folded into the Special Branch of the Metropolitan Police.[14] In addition to the Special Irish Branch, the British government had also established a military intelligence unit during the Boer War. The Field Intelligence Division (FID), a creation of the War Office, experienced countless setbacks during the war.[15] The FID not only suffered from under-staffing, but the intelligence reports they wrote were often neglected by the army in the field. They succeeded in distributing new and more accurate maps to officers and successfully predicted the number of Boer troops.[16] Despite some initial successes during the Boer War the FID was shut-down in 1904 following a parliamentary hearing.

---

[12] Andrew, *Her Majesty's Secret Service,* 18. I suppose it should not come as a surprise that the Irish played an intricate role in the foundation of the British intelligence organization. It is, however, a unique part of the “foundation myth” of British intelligence that often gets overshadowed by the UK-German arms race.

[13] *Ibid.*, 17.

[14] *Ibid*., 19.

[15] *Ibid.*, 28-29.

[16] *Ibid.*, 29.

Although the British had attempted to start intelligence organizations before World War I, it was not until the creation of the Secret Service Bureau that the British government would take its first firm step towards the creation of a permanent intelligence organization. The Secret Service Bureau was founded amidst what Keith Jeffrey dubbed "spy fever."[17] The popularity of William Le Queux's novels *The Invasion of 1910, England's Peril: A Story of the Secret Service, The Great War in England, The Bomb Makers, The Invasion* and *Spies of the Kaiser: Plotting the Downfall of England* whipped the British population into invasion frenzy.[18] *The Invasion of 1910*, serialized in the *Daily Mail* throughout 1906, increased the circulation of the paper by 80,000 copies.[19]

The threat of German invasion went hand in hand with the image of German spies that LeQueux generated. In his novel *The Bomb Makers*, LeQueux describes one of the protagonists as "an enemy alien, whose plans were maturing in order to assist a great and desperate conspiracy by the secret service of the German Fatherland."[20] LeQueux's attitude concerning his works was quite serious. He regarded his writing as an exercise of his duty. In the preface to *The Invasion* (published 1905) LeQueux recounts how he consulted with Earl Roberts in order to prepare for writing the book. In fact, Roberts encouraged LeQueux to write the book in the first place.[21] Roberts, a towering imperial personality who had more honors than letters in his name, was incredibly popular due to his command postings in India and the Boer war.[22] In addition to consulting with Roberts, LeQueux travelled "the whole of England from the Thames to the

[17] Keith Jeffrey, *The Secret History of MI6,* (New York: Penguin, 2010), 2-5.

[18] Jeffrey, *The Secret History of MI6*, 4-5; Andrew, *Her Majesty's Secret Service*, 34-35; Jeffrey-Jones, *In Spies We Trust*, 14.

[19] Jeffrey-Jones, *In Spies We Trust*, 14.

[20] William LeQueux, *The Bomb Makers: Being some Curious Records concerning the Craft and Cunning of Theodore Drost, an enemy alien in London, together with certain Revelations regarding his daughter Ella*, *http://www.gutenberg.org/files/41132/41132-h/41132-h.htm*. (accessed 4 August 2014)

[21] LeQueux, *The Bomb Makers*; Niall Ferguson, *The Pity of War*, (New York: Basic Books, 1999), 6-7.

[22] Frederick Sleigh Roberts, Oxford Dictionary of National Biography, http://www.oxforddnb.com/view/article/35768?docPos=1 (accessed 17 August 2014)

Tyne" in order to properly describe and create the fictitious invasion.[23] LeQueux reflected "that the experts and myself will probably be condemned as alarmists and denounced for revealing information likely to be of assistance to an enemy goes without saying."[24] This statement reflects LeQueux's attitude of self-worth. He was no mere writer, but an expert in the possibility of invasion. LeQueux was not looking to simply entertain, but to inform. His works were to serve as cautionary tales instead of adventurous entertainment. He wrote "To arouse our country to a sense of its own lamentable insecurity is the object of this volume."[25]

LeQueux's work may not have been regarded with such seriousness had it not been supported by both politicians and the print media. At the end of the prologue in *The Invasion*, Earl Roberts quoted his own address to House of Lords on 29 November 1905: "The catastrophe that may happen if we still remain in our present state of unpreparedness is visibly and forcibly illustrated in Mr. Le Queux's new book which I recommend to the perusal of everyone who has the welfare of the British Empire at heart."[26] An endorsement from a high-level member of parliament and national hero only reinforced, if not cultivated, the sense of invasion paranoia. According to Lord Roberts, LeQueux's work was an indispensable instruction manual for the vigilant, patriotic Briton. LeQueux's novels, coupled with political support, were only further heightened by the response of newspapers throughout the country.

It should be noted that LeQueux was not the only writer churning out invasion and spy literature. Authors such as Headon Hill, A.C. Curtis, Erskine Childer, R.W. Cole, Walter Wood, and countless others created their own elaborate and sensational plots about a possible

[23] LeQueux, *The Invasion*. I do not suppose that LeQueux ever thought that such in-depth research could possibly have been used as a reference for any real German plots against the United Kingdom.
[24] LeQueux, *The Invasion*.
[25] *Ibid.*
[26] *Ibid.*

invasion.[27] The number of spies in these schemes fluctuated from three-hundred to 40,000 to 290,000.[28] The method of attack was also varied: the German spies attacked from within Britain, bombed London from gigantic Zeppelin airships, or attempted to decimate the British fleet in the English Channel. While LeQueux's works garnered respect from political figures, many of his contemporaries were satirized and ridiculed by *Punch* magazine and other British humorists. Niall Ferguson wrote, "It should be stressed that many contemporaries found the more febrile of the scaremongers simply laughable."[29] LeQueux's works and opinion, however, were the only ones taken seriously. "The extraordinary point," writes Ferguson "is how seriously the scaremongers' allegations were taken by senior British officials and ministers."[30] The contradiction that Ferguson identifies is a puzzling one. Why was it that the satirists and humorists of Britain—a group that was educated, and sometimes affluent—could see the ludicrous nature of these plots while senior military officials and top-ranking politicians could not?

The rumors of there being German spies operating throughout Britain were greatly unfounded according to modern scholars. Christopher Andrew states that the Germans were running "an inefficient network of poorly paid and clumsy part-time agents."[31] This description pales in comparison with the colorful, malicious, and maniacal portrait cultivated by LeQueux. The sense of paranoia was so present that Prime Minister Herbert Asquith ordered the Committee on Imperial Defense (CID) to look into the feasibility of a foreign invasion.[32] Edwardian media was often littered with tales of German infiltration, often portraying German

[27] Ferguson, *The Pity of War,* 1-3.
[28] *Ibid*., 2-3.
[29] Ferguson, *The Pity of War,* 5.
[30] *Ibid*., 13.
[31] Andrew, *Her Majesty's Secret Service*, 54-55.
[32] Jeffrey, *The Secret History of MI6,* 4-5.

spies penetrating the sacred institutions of the picturesque English countryside communities—pubs, bed and breakfasts, village greens—in order to gather intelligence, implanting themselves the heart of Britain. Beginning in 1907 the War Office began receiving more and more reports of suspected German spies. Christopher Andrew states that between 1907 and early 1909 there were 76 cases of such activity reported to the War Office.[33]

Newspapers were the last, and perhaps most influential factor in cultivating the sense of invasion paranoia in Great Britain. The print media throughout Britain played the chorus to Lequeux's and Robert's invasion-crazed dialogue. The newspapers fed directly off LeQueux's novels. This reaction is evident in an article written by Reginald Glossop in *The Daily Mail* on 14 November 1906.[34] "In my opinion," wrote Glossop "Germany would never adopt the tactics displayed in the pages of William LeQueux's book on the invasion of 1910." Glossop did not negate the theory of invasion outright, instead he officers an alternative scheme in which a group of "mechanics, trained soldiers, and motor experts" create havoc and initiate sabotage throughout the England.[35] Such a plan would include the destruction of Britain's infrastructure and a deep infiltration of British institutions, such as the Royal Navy. Glossop's article takes the form of an imaginary briefing delivered by the German commander-in-chief to his three hundred best spies on the eve of the fictitious invasion. Glossop concludes the article by issuing a statement of support for Earl Roberts: "I know for a fact that that brave and chivalrous solider, Lord Roberts, possesses more foresight than any general England ever had—or has—should succeed in manning the entire island."[36]

---

[33] Andrew, *The Defense of the Realm*, 15-17.

[34] Reginal Glossop, "Invasion of Britian: Imaginary Conversations and Instructions of the German General Staff," *The Daily Mail*, 14 November 1906. Accessed from the Newspaper Archive at the British Library.

[35] *Ibid.*

[36] *Ibid.*

The combination of LeQueux's novels, support from political figures such as Lord Roberts, and the enthusiastic involvement of print media led to increased interests in alien persons in Great Britain. Seven months prior to the publication of Glossop's article, a letter sent to Colonel Warde at the Home Office complained about "a person who speaks English with a strong German accent, and who has…been devoting himself with great care to the preparation of maps in your Country." [37] The author of the note continues to suggest that Colonel Warde "have him [the stranger] traced and watched in such a way to make him uncomfortable."[38] The intelligence community would soon run into a problem, however. The author of the letter also mentions that "There is of course no power to stop him [the stranger]." After the publication of LeQueux's novel and the public support of Lord Roberts, the newspapers were filled with stories of spies in Britain. The British government was faced with a substantial problem: how to legally monitor and track suspicious persons? Without an existing legal precedent, the government was unable to conduct anti-espionage activities in the manner they desired. In order for the British government to catch the legions of spies lurking in the countryside, they could not take the time to collect and build a legal case against any suspicious persons. The government needed to be capable of seizing any suspect and hold them without readily available evidence, seizure without charge.

1909 was a pivotal year for the development of British intelligence. The year began with a flurry of newspaper stories concerning a possible German spy plot. A story ran on 2 January in *The Aberdeen Daily Journal* about the possibility of a German invasion. The reporter wrote "There is another matter of very grave importance which cannot be too vividly brought before

[37] National Archives (UK) HO 317/43 Letter to Colonel Warde, London, 12 May 1906.
[38] *Ibid.*

the public—that is the element of surprise."[39] The "element of surprise" mentioned by the reporter would take the form of either a swift destruction of the Royal Navy or by Zeppelin raids. On 27 January another story broke in several papers about the possibility of five to six thousand German spies in England and Scotland. The *Nottingham Evening Post* reported that the German spies numbered 6,000 and were divided into two divisions responsible for spreading chaos throughout the industrial centers of the country. On the same day the *Dundee Courier* warned that the "whole country's defences are known to Berlin."[40] Stories of this nature began to appear with some regularity in newspapers until the beginning of World War I. The government began to take notice, the CID acted. It seemed that the British government was no longer capable of ignoring the possibility—no matter how real or imagined—of German invasion, or possible infiltration by German spies.

The sub-committee of the CID met three times throughout 1909 and arrived at a startling conclusion: the British were incapable of gathering intelligence coherently at home and abroad. The sub-committee decided to combat this problem by establishing the Secret Service Bureau (SSB). The establishment of the SSB was shrouded in such secrecy that only a single copy of the order was made.[41] The War Office, acting under orders from the CID, appointed the Honorable A.E. Bethell, the Director of Naval Intelligence (DNI), to find a suitable candidate to head up the new agency. He drafted a short letter to Commander Mansfield Cumming. Cumming had led a

[39] "General Russell on Possible Invasion," *The Aberdeen Daily Journal*, 2 January 1909. Accessed from the Newspaper Collection at the British Library.

[40] "German spies in Scotland: Whole Country's Defences are Known to Berlin, System of Espionage Exposed." *Dundee Courier*, 27 January 1909. Accessed from the Newspaper Collection at the British Library.

[41] Andrew, *The Defense of the Realm*, 20-21.

distinguished military career and had come out of retirement in 1898 to work on the boom defenses at Southampton.[42] The letter read:

> "My dear Mansfield Cumming. Boom defence must be getting a bit stale with you and recent experiments with Ferret rather discounts yours at Southampton. You may therefore perhaps like a new billet. If so, I have something good I can offer you and if you would like to come and see me on Thursday about noon I will tell you what it is."[43]

The Bethell letter, cryptic and enigmatic as it may be, would become part of the bedrock that made up the foundation myth of British intelligence. The formal foundation of the SSB was only half the battle. The burgeoning British intelligence community was soon going to be given a boon from Parliament.

In addition to the establishment of the Secret Service Bureau, the intelligence community was bolstered further by the passage of the Official Secrets Act of 1911. This was the legislation that could enable the newly formed SSB to carry out their task of rooting out possible spies. The passage of this act would have wide implications lasting well into the twenty-first century. The 1911 bill was a revision of the 1889 act of the same name, which was deemed inadequate by the CID.[44] The bill states that any person who attempts to aide in any activity "prejudicial to the state or interest of the state," will automatically face prosecution from the government. If the accused was found guilty of felony they "shall be liable to penal servitude for any term not less than three years and not exceeding seven years."[45] More importantly, the bill decreed that the state did not have to prove guilt, but instead the individual on trial had to provide proof of their own

---

[42]*Ibid.*, 25.

[43] "Bethell letter." 10 August 1909, https://www.sis.gov.uk/our-history/bethell-letter.html. Accessed 18 March 2014.

[44] Andrew, *Her Majesty's Secret Service*, 63.

[45] "Official Secrets Act 1911." 22 August 1911 http://www.legislation.gov.uk/ukpga/Geo5/1-2/28/contents. Accessed 21 March 2014.

innocence.[46] This blatant suspension of *habeas corpus* upset parliamentary liberals, including Sir Alpheus Morton, who believed the bill directly contradicted the Magna Carta.[47] The act undoubtedly violated the basic principles of any ideals concerning the freedom and rights of individuals. It flew in the very basic principles that constituted Common Law.

In addition to suspending *habeas corpus,* the Official Secrets Act also restrained freedom of speech in Britain. It was no longer just spies who faced prosecution, but also journalists. The result was the practice of wide spread self-censorship amongst the journalistic community. A prime example of this can be found in Hugh Cleland Hoy's book *40 O.B. or How the War was Won,* which was published in 1932, only 21 years after the passage of the act. Hoy had worked as a codebreaker during World War I. He wrote "The Official Secrets Act is far-reaching, and I am also bound by personal loyalty to the service, to my superiors in that service, and to the promptings of humanity and the demands of social obligation. So in making this compilation I have had to remember—and also to forget."[48]

The bill would not only change how the intelligence community was able to conduct its work, but how it would be chronicled, or perhaps more importantly, not chronicled. The British press would self-censor itself for many decades following the passage of the act, and those journalists who stepped out of line were promptly prosecuted. The cohesion of confidentiality between the government and the press is an indication of how seriously the powers-that-be cherished secrecy. Silence in the name of national security became a rallying cry of both British spies and journalists. For the most part this gentlemen's agreement remained true, but there were still instances in which persons violated the Official Secrets Act, sometimes publicly. The

[46] *Ibid.*
[47] Andrew, *The Defense of the Realm,* 39; Idem, *Her Majesty's Secret Service,* 64-65.
[48] Hugh C. Hoy, *40 O.B. or How the War Was Won* (London: Hutchinson & Co., 1932), 20.

government reactions, surprisingly, differed drastically. The act could, in theory, apply to any British citizen, and result in the stripping of their basic rights. But not every violation was treated equally.

Hoy may have had the self-discipline to not reveal secrets in his book, but other figures were not so tight-lipped. In two different instances following both the passage of the Official Secrets Act of 1911and the First World War individuals openly broke the Act and were treated differently. The first of these noticeable violations occurred on 13 December 1927. On this date Alfred Ewing, a former high-ranking member of Room 40, delivered a lecture to the Edinburgh Philosophical Institution about his war time work.[49] Within the lengthy speech Ewing revealed many secrets about Room 40. Some of the details of his war time work were leaked to press. The Admiralty took particular notice. O.A.R Murray, permanent secretary of the Admiralty, authored a memo three days following Ewing's address. "The publication of such information," wrote Murray in reference to the press' reaction "is prejudicial to the interests of the State, and is in fact contrary to the provisions of the Official Secrets Act of 1911 and 1920."[50] The Admiralty pointed out Ewing's violation, but did not seek to discipline him in any way. This came from the fact that while Ewing revealed specifics of Room 40's operations and several classified incidents such as the sinking of the *Magdeburg* and others—to be elaborated on later in this paper—he refrained naming any of his fellow codebreakers by name. It was this act of self-censorship and Ewing's reputation that saved him from any serious repercussions. The fact remains, however, that by acknowledging the existence of Room 40 Ewing violated the Official Secrets Act. It was Ewing's speech that allowed Hoy to write his book in the first place.

---

[49]NA ADM 1/23899, Copy of speech given by Alfred Ewing entitled "Some Special War Work: A Lecture to the Edinburgh Philosophical Institution," manuscript, Edinburgh, 13 December 1927.

[50] NA HW 3/182Letter by O.A.R Murray, London, 16 December 1927.

The second incident took place seven years following Ewing's address in Edinburgh, when Mr. Edgar Lansbury was arrested for violation of the Official Secrets Act of 1911.[51] On 24 March 1934 Lansbury was visited by police detectives at his residence at No.7 Weymouth Avenue in London. He had recently written a biography of his late father entitled *George Lansbury: My Father*. George Lansbury had held the position as First Commissioner of Works during the early 1930s.[52] Within the text of the work Edgar Lansbury quoted "verbatim from two secret Memoranda" from Cabinet Office meetings that his father had attended.[53] By reading and publishing these memorandums Edgar Lansbury violated section 2.2 of the Official Secrets Act. Upon being informed of his violation, Lansbury claimed "I did not know it was an offence at the time." Lansbury was taken to court and fined £10 per summons for a total of £20, plus twenty-five guineas in court costs.[54] In addition to this, Lansbury's misdeeds were covered in-depth in *The Daily Telegraph*.[55] Although the fine of £20 was minimal when compared to a prison terms, it should be noted that the excerpts published were small. Ewing's speech revealed much more in the way of national secrets, but he did not quote from secret documents in his possession. It was Ewing's reputation that had saved him from formal charges.

Rhodri Jeffrey-Jones surmises that the passage of the Official Secrets Act was also a class-driven. Jeffrey-Jones writes the bill "was a step consistent with the emergence of an intelligence establishment based on the premiss that those of 'officer' status could be trusted, but lower-order 'spies' had to be subject to vigilant discipline."[56]In essence, the partial motivation behind passing the bill was to cauterize the leaking of delicate information. In the eyes of the

[51] MEPO 3/1106, Materials related to the Landsbury Case, London, March 1934.
[52] *Ibid.*
[53] *Ibid.*
[54] *Ibid.*
[55] *Ibid.*
[56] Jeffrey-Jones, *In Spies We Trust,* 22.

privileged classes, who had enjoyed a ruling monopoly for centuries, the lower classes lacked the loyalty and personal steadfastness to be trusted. As mentioned before, Alfred Ewing openly violated the Official Secrets Act, but faced no repercussions in his lifetime. Despite the obvious problems with this world view—Jeffrey-Jones uses the example of the gabbing Edward VII as a prime example of a loose-lipped member of the upper-class—Jeffrey-Jones does make a compelling point that will be addressed in part later in this chapter when I discuss the recruiting of intelligence personnel.[57] No matter why it was initially created, the Official Secrets Act of 1911 was fundamental in providing a legislative basis on which the intelligence community could base its actions. The intelligence community now had the ultimate backing to carry out their plans.

British intelligence would face its first great trial during the World War I. If Irish bomb threats, the Boer War, and threats of German spies had led to the temporary interest in intelligence gathering, than World War I was the sole catalyst in the sustaining of a permanent organization. Following the assassination of Franz Ferdinand and a very intense July, Great Britain declared war on Germany at midnight on 4 August 1914. Room 40 was established within ten days of the declaration of war. The main focus of Room 40 was cryptography, the studying and breaking of codes and monitoring German wireless radio traffic. Britain, like most of the other European nations, had not established a codebreaking operation. Paul Gannon refers to the beginning of Room 40 as "a truly British tale of bumbling amateurishness that just about helps the country pull through in its hour of crisis."[58] The origins of Room 40 begin with Alfred Ewing, the University of Edinburgh educated engineer. Ewing was an intelligent Scotsman who

---

[57] Jeffrey-Jones, *In Spies We Trust,* 22.
[58] Gannon, *Inside Room 40,* 21.

had held teaching posts at the universities of Tokyo, Dundee, and Cambridge.[59] In addition to his teaching duties, Ewing busied himself by writing encyclopedia articles, serving as an expert witness in court cases, and providing guidance to large industrial construction projects.[60] In 1902 Ewing was appointed Director of Naval Education. He was incredibly successful, rising in the ranks of the admiralty rapidly. With this strange combination of skills, it was only natural that he would lend himself to codebreaking.

On 4 August Rear-Admiral Henry “Dummy” Oliver, Director of Naval Intelligence, received a number of coded wireless signals intercepted by an Admiralty radio station.[61] He quickly decided that Ewing would be the most suitable candidate to head up a radio analysis unit. Oliver and Ewing met later that day. Ewing later recalled that “that he [Oliver] said he had no one to deal with these intercepts: would I take the matter up and see if I could make anything of them?”[62] Ewing had previously had experience with radio communications, having patented an electro-magnetic wave detector that he referred to as “a rather futile machine.”[63] Whether or not the machine was futile, Ewing seemed the man for the job. “Of course I said I should try,” wrote Ewing later “it was a moment when one grasped at even the most unpromising chance of being useful.”[64] Following Ewing’s acceptance of the position all intercepted messages were addressed to him at the admiralty building.

The first task Ewing completed at his new post was the setting up a wide network of wireless radio stations. The admiralty started with two such stations, but Ewing commandeered

[59] Andrew, *Her Majesty’s Secret Service,* 86.
[60] Gannon, *Inside Room 40*, 29.
[61] Andrew, *Her Majesty’s Secret Service,* 86.
[62] NA ADM 1/23899, Ewing speech, Edinburgh, 13 December 1927.
[63] NA, ADM 1/23899; Mavis Batey, *Dilly: The Man Who Broke Enigmas.* London: Biteback, 2009, 13.
[64] NA, ADM 1/23899.

several others manned by the Marconi Wireless Telegraph Company and the Post Office.[65] These were the only facilities capable of monitoring German wireless radio traffic. Such facilities were key in monitoring German communications. According to Ewing these stations acted “as official eavesdroppers to bring grits to the mill of the deciphering staff, intent night and day that not a whisper of the enemy might be missed.”[66] Following the seizure of these stations the amount of intercepted radio traffic increased substantially. Ewing wrote that “the stream [of messages] swelled till the number of messages that came addressed to “Ewing, Admiralty” sometimes exceeded 2000 a day.”[67] The entire starting process of the codebreaking department was shaky, and the progression seemed off the cuff, but Ewing and his merry band of codebreakers were making necessary progress. Ewing continued to lake logical steps in establishing the new enterprise.

The next task Ewing was charged with was the recruiting of men to join the codebreaking group. He specifically sought out linguists from the naval language schools at Dartmouth and Osborne.[68] Alfred Dillwyn Knox and Alistair G. Denniston would become an integral part of Room 40, and its successor, the Government Code and Cypher School (GC&CS). Knox was born into a talented group of children, the second of four boys.[69] The Knox brothers were certainly an accomplished lot; Monsignor Ronald Knox was a writer and translator of the Bible, Wilfred was an Anglican priest and classicist who also achieved great prominence as a writer,

---

[65] Mavis Batey, *Dilly: The Man Who Broke Enigmas.* London: Biteback, 2009, 13.
[66] NA, ADM 1/23899.
[67] *Ibid.*
[68] Andrew, *Her Majesty’s Secret Service,* 87.
[69] Penelope Fitzgerald, *The Knox Brothers*, (London: Flamingo, 1977), xi.

and Edmund was a celebrated satirist who was the editor of *Punch* magazine from 1932-48 and had been deemed the funniest man in England at one point in time.[70]

A.D. Knox was educated at Eton and then matriculated to King's College, Cambridge, where he distinguished himself as an excellent classical scholar under Walter Headlam.[71] When Headlam died unexpectedly died in 1908, Knox took over his fellowship at King's and toiled for years to complete Headlam's commentary on Herodas' poem *Mimes*.[72] In early 1915 Knox was recruited to join the rag-tag, experimental crew in Room 40.[73] He fit the profile perfectly. Knox's eccentricities made him a character in a comical work about Room 40 titled *Alice in ID25* in which Alice—of *Alice in Wonderland* fame—finds herself lost in the deep piles of decoded radio messages in Room 40. Frank Birch, an Old Etonian, fellow at King's and author of *Alice in ID25*, dubbed Knox "Dilly the Dodo."[74] Much of the laughter surrounding Knox stemmed from his preoccupation with baths. Knox was lodged in Room 53 of the Old Admiralty Building, which was the only room fitted with a bathtub. Whether or not Knox demanded these quarters is unknown, but he certainly used the bathtub often. According to Christopher Andrew "Dilly did some of his best work for Room 40 lying in a bath in Room 53, claiming that codes were most easily cracked in an atmosphere of soap and steam."[75] For all of his eccentricities and bath-related quirks, Knox became a fixture of the British codebreaking community. Knox eventually was named head of GC&CS and oversaw the cracking of the Enigma code during World War II.

A.G. Denniston would also become an essential part of British codebreaking in World War II. In many ways he and Knox shared the same background. Denniston was educated at

---

[70] *Ibid.*
[71] John Richmond, "Classics and Intelligence." *Classics Ireland*. Volume 9 (2002).
[72] *Ibid.*
[73] Batey, *Dilly*, 13.
[74] *Ibid.*, 95.
[75] Andrew, *Defence of the Realm,* 94.

Bowden college, where he was praised as an excellent student. Instead of attending either Oxford or Cambridge, Denniston attended the Sorbonne and Bonn University.[76] Denniston was also a talented athlete, playing hockey for Scotland in the 1908 Olympics.[77] In late 1914 he was enlisted by the Admiralty for Room 40 due to his exceptional German and French linguistic skills.[78] It was men such as these that were gathered together to help establish Britain's first codebreaking group since the Foreign Office's deciphering branch in 1844.[79]

The blueprint for recruiting codebreakers would not change much from one world war to another. Linguists, classicists, and mathematicians were all recruited into Room 40. Early in the war all six fulltime codebreakers worked in the same cramped office. There was little room the men had to work in shifts around the clock. Three of the codebreakers were trained mathematicians who spoke and read virtually no German whereas the three linguists and classicists spoke it fluently.[80] The balance between the two types of minds would eventually be perfected and duplicated during the Second World War. During the First World War Room 40 became a repository for several distinguished scholars.

The recruitment was concentrated primarily at gifted students from Oxford and Cambridge. William F. Clarke, who worked as a codebreaker during both world wars, later wrote about the formation of Room 40: "Nearly all were civilians enlisted from Osborne and Dartmouth masters, dons from universities nearly[y] all King's College, Cambridge."[81] From Cambridge Room 40 recruited ancient historian Franck Adcock, theologian Reverend William

[76] Robin Denniston, *Thirty Secret Years: A.G. Denniston's work in signals intelligence, 1914-44*. Great Britain: Polperro Heritage Press, 2007, 11-12.
[77] *Ibid.*
[78] *Ibid*.
[79] Christopher Andrew, "Codebreaking and Foreign Offices: The French, British, and American Experience," in Andrew and Delks, eds., *The Missing Dimension*, 43.
[80] Andrew, *Her Majesty's Secret Service*, 88.
[81] NA, HW 3/3. Manuscript entitled *History of Room 40 O.B.* written by William F. Clarke, London, 2 July 1951.

Montgomery, German linguist Edward Bullough, E.C. Quiggin, C.W. Hardisty, and W.H. Brufford. Oxford was also well represented, contributing Greek vase expert John Beazley, classicist Ernest Harrison, Leonard Willoughby, and Neville Forbes. In addition to the Oxbridge fellows, there were several other leading authorities from institutions in Leeds, Dublin, Birmingham, and Belfast.[82] Universities would prove to be fertile recruiting grounds for both Room 40 and GC&CS during World War II. In fact, many of those men recruited during the First World War returned to work at GC&CS during the Second.

The impressive list of academics recruited into Room 40 seems to strengthen the argument put forth by Jeffrey-Jones that "those of 'officer' status could be trusted" and the lesser classes could not be trusted.[83] Ewing's decision to draw from the ranks of Oxbridge's professorial could have very well been class driven, but I believe the decision may not have been so consciously socially motivated. It only stands to reason that Ewing, a prominent academic in his own right, would find academics to be the most suitable for the job. Academics, especially those trained in the humanities, would have certainly been well-versed in analytical thought and often fluent in German or other languages. Familiarity with languages, various grammatical structures and syntax made academics a viable, if not ideal, candidate for the analysis of code and messages. Barbara Tuchman referred to the men in Room 40 as "university dons, barristers, linguists, accountants with a flair for mathematical pattern, all men who went into battle against the ciphers with a zest for the intellectual challenge."[84] Due to the new nature of the discipline, the first British codebreakers needed only the intellectual capabilities and the drive to pioneer the new field.

---

[82] Andrew, *Her Majesty's Secret Service*, 96.
[83] Jeffrey-Jones, *In Spies We Trust*, 22.
[84] Barbara Tuchman, *The Zimmerman Telegram*, (New York: The Macmillan Company, 1958), 12.

It should be noted that at first, the idea of having a codebreaking section was looked at with some skepticism. Eventually the group was able to expand, moving into Room 40 of the Old Admiralty Building.[85] Winston Churchill has received much of the historiographic credit for placing real value on signals intelligence (SIGINT). Christopher Andrew states that "Churchill was the first British minister to grasp the potential importance of sigint."[86] It was Churchill who had been responsible for pushing the Official Secrets Act through Parliament. He was one of the single most ardent supporters of the bill.[87] Later, as First Lord of Admiralty, Churchill had a very keen interest in the development of Room 40. On 11 October 1914 Churchill addressed the memo to Henry Oliver, instructing him to appoint someone—eventually Ewing—to head the new codebreaking section. This message is often referred to as the "Room 40 Charter," although Paul Gannon has voiced the opinion that it was little more than a formal memo.[88] It cannot be ignored that Churchill nurtured the new organization by supporting it and providing funds for growth.[89] Churchill's early interest in intelligence and codebreaking also led to the systematic "logging" of codes in a systematic and chronological fashion, similar to the keeping of a ship's log.[90]

Despite the hastily establishment of Room 40 at the beginning of the war, the collection of university dons and naval personnel managed to play a vital part in the war from an early stage. In October the 30 members of this new outfit set up headquarters in the Old Admiralty building. William F. Clarke wrote that the group was "housed in three rooms of the Old building,

---

[85] Batey, *Dilly*, 14.
[86] Andrew, *Her Majesty's Secret Service,* 90.
[87] Andrew, *The Defense of the Realm*, 20.
[88] Gannon, *Inside Room 40*, 82.
[89] *Ibid*., 84.
[90] Mavis Batey, *Dilly*, 16.

one of which was a small bedroom with one bed, infested by mice."[91] Poor conditions did not deter the small group from getting to work. Already the war had been underway for two months and there was work to do. Since the declaration of war, several key events had already taken place.

Patrick Beesly states, "The foundations of Room 40's tremendous success were laid swiftly but largely in the first twelve weeks of the war."[92] The first of these successes was the severing of German telegraph cables. By cutting the underwater cables, Germany was virtually isolated from communicating with its colonies and embassies abroad.[93] With their telegraph lines severed, the Germans had no choice but to rely on wireless radio transmissions. Secondly, the British were able to secure physical copies of all three of Germany's naval codes.[94] By obtaining the copies of these codes the British enabled themselves to crack all of the coded wireless radio messages. It was a distinct advantage for the British from the outset of the war. The first codebook was seized off the coast of Australia on 11 August 1914.[95] The *Hobart,* a German-Australian steamship, was boarded by Captain J.T. Richardson of the Royal Australian Navy (RAN) under the guise of inspecting the ship for quarantine.[96] Richardson's search was purposefully unaggressive, as he hoped the captain of the *Hobart* would reveal his secret documents when he tried to destroy them. Richardson found the German captain attempting to destroy the confidential documents early in the morning.[97] On 9 September the RAN board in

---

[91] NA, HW 3/3., Clarke manuscript.

[92] Patrick Beesly, *Room 40: British Naval Intelligence 1914-18*, (New York: Harcourt Brace Jovanovich, Publishers, 1982), 2.

[93] *Ibid.*, 2-3.

[94] *Ibid*.

[95] *Ibid*., 3.

[96] *Ibid.*

[97] *Ibid.*, 3-4.

Melbourne informed London of the successful seizure, a copy was made and London received it in October.[98]

The second set of codebooks was acquired when the Russian navy destroyed the German light cruiser *Magdeburg* on 25 August.[99] The *Magdeburg* ran aground in the Gulf of Finland and was decimated by two Russian destroyers.[100] A German sailor escaped the sinking ship and died with the codebooks in hand.[101]Ewing later reflected on what he called a "priceless acquisition," writing "To save the book from the enemy, was, one may conjecture, the impulse of a gallant man facing death; but, if that was his purpose, it was frustrated. The sea gave up its dead, and, with the dead, it gave up the book so loyally preserved."[102] The Russians discovered the codebooks and promptly sent them to the British.[103] This shows a rare instance of Allied cooperation during the war. Patrick Beesly referred to it as the Russians showing "uncommon good sense in a spirit of co-operation which was not repeated in World War II."[104] There were three types of radio codes the Germans used. The *SKM – Signalbuch der Kaiserlichen Marine* (Signal Book of the Imperial German Navy) – was taken off the *Magdeburg*.[105] The *SKM* was a "German navy signaler's bible" according to Paul Gannon.[106] The *SKM* contained a large list of three letter code words and the meanings that aided the British significantly at the beginning of the war. The second code, *Handelsschiffsverkehrbuch* (Commercial Ship Communication Book) or *HKM*, was primarily used by German merchant ships and Zeppelins used for naval

[98]Beesly, *Room 40*, 4.
[99] NA, ADM 1/23899: Copy of speech given by Alfred Ewing entitled "Some Special War Work: A Lecture to the Edinburgh Philosophical Institution," Edinburgh, 13 December 1927; NA, HW 3/3. Manuscript entitled *History of Room 40 O.B.* written by William F. Clarke, manuscript, London, 2 July 1951.
[100] *Ibid.*
[101] *Ibid*.
[102]*Ibid*.
[103] *Ibid*.; Jeffrey-Jones, *In Spies We Trust,* 23.
[104] Beesly, *Room 40*, 5.
[105] Gannon, *Inside Room 40,* 47-48.
[106]*Ibid.,* 48.

reconnaissance.[107] The third code, the *Verkehrsbuch,* (Communication Book), or *VB,* was employed by submarines, small patrol craft, and foreign embassy officials.[108] Each code was uniquely used by different branches of the German navy and helped the British codebreakers in Room 40 significantly.

There was a plethora of information contained in the codebooks, including the navigational grid system the Germans used to coordinate naval movements.[109] Although there were some initial problems in applying the information from the recovered codebooks to the monitored radio traffic, the codebreakers in Room 40 were monitoring German radio traffic with regularity by November 1914.[110] The remarkable aspect of codebreaking during the First World War, and what made different from Room 40's predecessors at GC&CS was that all of the codebreaking done by the men in Room 40 was done completely by hand. Ewing later wrote that it was "Fleet-Paymaster Rotter, who combined a thorough knowledge of German with a remarkable talent for solving such conundrums" who broke the German naval codes. It took Rotter a few days of intensely studying the captured cooks to break down the pattern in the codes. The Germans did not alter their encryption process until May 1917.[111]

The seizure of the three various codebooks would give the British codebreakers in Room 40 a distinct advantage for the remainder of the war. These early successes enabled them to successfully track key German naval and army movements. The focus of the German navy and the British codebreakers following it would change rapidly. By 1915, the Germans decided to

[107] Beesly, *Room 40,* 3-4.
[108] Gannon, *Inside Room 40,* 54.
[109] NA, ADM 1/23899, Ewing speech, Edinburgh, 13 December 1927.
[110]*Ibid.*.
[111] *Ibid*.

focus primarily on submarine warfare.[112] Room 40 would continue to work out the kinks of the very complex task-at-hand. The crowning achievement of Room 40 would be the interception and decoding of the infamous Zimmerman Telegram on 16 January 1917.[113] The telegram first came across Knox's desk, but according to Nigel de Grey, Knox's "knowledge of German was at the time too slender for him to tackle any difficult passages in telegrams."[114] DeGrey and Knox both worked on the message steadily all morning and by noon they had a working version.

DeGrey and Knox knew ascertained from their skeletal translation that the message was important. They immediately ran the message down to Admiral "Blinker" Hall. DeGrey recalled the meeting between the three of them later. He wrote:

> "I was young and excited (so incidentally was Dilly Knox) and I ran all the way to his room, found Seracold (his P/A) alone and Blinker free. I burst out breathlessly "Do you want America in the war Sir?" "Yes, why?" said Blinker "I've got a telegram that will bring them in if you give it to them". As may be seen I had all the confidence of my years."[115]

DeGrey and Knox's confidence in the preliminary translation got matters moving in the British government. As soon as they convinced Hall of the message's legitimacy they began speaking with Arthur Balfour, the Secretary of State for Foreign Affairs, about how to best proceed with the matter delicately. If they botched the handling of the Zimmerman Telegram, then the British could possibly reveal the existence of Room 40 and the fact that the British had violated U.S.-Swedish neutrality.[116]

[112] Jeffrey-Jones, *In Spies We Trust*, 20-21.
[113] Tuchman, *The Zimmerman Telegram*, ix.
[114] NA HW 3/77, "Zimmerman Telegram: A footnote to Friedman's Account" by Nigel de Grey, London, 31 October 1945.
[115] *Ibid*.
[116] NA HW 3/179, Memorandum regarding the Zimmerman Telegram, London, 24 February 1917.

The Zimmerman Telegram soon left Room 40 and began its long journey through the different halls of the British, American, and Mexican governments. There is no need to describe how the telegram made its hands of the American government, because Room 40's contributions were in the beginning. This single message would change the outcome of the entire war. The Zimmerman Telegram exposed an ambitious and imaginative plot that would eventually bring the United States out of the daze of splendid isolationism and into the demanding forefront of a burgeoning world power. The cracking of the Zimmerman Telegram remains the greatest historical legacy of Room 40.

All government organizations are created for a reason, for strong contextual reasons. The creation of these groups is directly related to the atmosphere of the time period in which they are fashioned. Rhodri Jeffrey-Jones writes that "Once the war started, there was a sudden, mushroom expansion in intelligence personnel activities."[117] The invasion craze of the Edwardian era led to the creation of the Secret Service Bureau in 1909, the Bureau was given legislative grounds for operation with the passage of the Official Secrets Act of 1911, and the outbreak of First World War. The outbreak of war galvanized Britain into sustaining an intelligence community. No longer could Great Britain be satisfied with creating ad-hoc intelligence agencies that would address specific conflicts or threats. It was the First World War that ensured the British would be able to eventually break the Enigma code over twenty years later.

Many of the practices used by the British twenty-one years later had been established during the First World War. Room 40 thrived on the recruiting of variously focused, but intelligent personnel who had a knack for problem-solving and relied on the analysis of physical intelligence. These were the foundations that the British would return to during the Second

[117] Jeffrey-Jones, *In Spies We Trust*, 20-21.

World War. The fundamental difference would be that circumstances would dictate that the British would have to rely on a mechanical approach to breaking the code.

In a broader sense, the militaries of Europe became devoted to the creation of an encryption system that could keep their messages secret. The First World War was the catalyst to the creation of the Enigma machine, and the organizations that would eventually break that code.

CHAPTER 3

THE CREATION OF THE ENIGMA MACHINE, BRITISH & POLISH RESPONSES TO THE MACHINE & CODE, 1918-39

"Aurum irrepertum"

—phrase meaning "gold discovered" used in letter by A.D. Knox

The First World War was vital for the creation of a British codebreaking organization, but it was the interwar period that witnessed the birth of the Enigma machine and code. The interwar years were a pivotal time period for the Germans. It was during this time that they were able to develop the intricate machine that would confound the British during the first few years of the Second World War. Much like the rise of the Nazi Party, the Enigma slowly grew throughout the twenties and came into maturation during the 1930s. The British were not the first to come in contact with the Enigma code. It was the Poles who would first attempt to and succeed in breaking it. This chapter will analyze the creation and progression of the Enigma code from interesting invention to coveted military tool, the growth of a Polish codebreaking unit, the Polish attempts and limited successes in breaking the Enigma code, British knowledge of the Enigma, the interaction between the Poles and other Allied powers on the eve of the Second World War, and the rebuilding of the British codebreaking organization in the early years of the war.

The Enigma machine did not begin life as a military tool. It was developed for commercial use immediately following the First World War by Arthur Scheribus, who sought to market the device towards banks and businesses.[118] Scheribus was a German inventor who established a small engineering firm in 1918 with the objective of creating a device capable of

[118]John Keegan, *Intelligence in Warfare: Knowledge of the Enemy from Napoleon to Al-Qaeda*, (London: Pimlico, 2004), 173.

both encrypting and decrypting messages.[119] Several attempts had been made earlier in the decade to create a device capable of this, but Scheribus was the first to succeed. It took him five years to perfect the design. In 1923 the first commercial Enigma model was made available for purchase.[120]

When the Enigma machine was first distributed each model came with an instruction booklet. The British obtained one of these instruction booklets in 1923 and later had it translated.[121] The author of the booklet wrote "By intercepting important dispatches battles have been won, by deciphering dispatches of foreign countries important political plans have been crossed; on the other hand, by the early and secret transmission of commercial messages great fortunes have been amassed."[122] The author could not have known how true the beginning of that sentence would be in subsequent years. Scheribus initially focused on the latter half of the statement, the amassing of vast fortunes. The booklet gave instruction on how to operate the machine, and also boasted that the machine was "essentially incapable of solution since the number of substitution alphabets produced by the machine is so great, and the variability with which the individual alphabets follow one another is so thorough that similarities do not occur within a period of some 1,000,000 letters."[123] This figure is already quite impressive, but the number of variables would grow substantially by the beginning of the war. As a potential tool for any business, the prospect of being able to send messages like this must have seemed too good to be true.

---

[119] *Ibid.*
[120] *Ibid.*
[121] NA HW 25/8, Enigma Instruction Booklet written in German, English translation attached, London, 1923.
[122] *Ibid.*
[123] *Ibid.*

The British began to take notice of the commercial Enigma too. As early as 2 June 1924 the British attempted to purchase an Enigma machine.[124] Lieutenants Hume and Dickinson, both serving in the embassy in Berlin, had inspected the machine parts in 1921.[125] By 1924 the Enigma machine had been purchased by the Italian Naval and Air Forces, the Czechoslovakian Foreign Office, the Swiss Post Office, and the Dutch Post Office.[126] The Japanese government was also negotiating the purchase of a machine. On 1 July 1924 Alistair Denniston, now serving as the Head of the newly formed Government Code & Cypher School, acknowledged that his department would inspect the machine and prepare a report on it.[127] The enigma machine was already impressing people in Britain. In a letter sent from the British Consulate in Amsterdam to Sir E.T.F Crowe in the Department of Overseas Trade in January 1925 , Henry Tom wrote that after inspecting the machine he found it "rather wonderful and even if the Government does not intend purchasing any I am sure that you would be interested to see them working."[128] This sentiment was later echoed in a report on the Enigma machine written in March 1926. The author of the report concluded that "Even should they be found unsuitable for service work I believe a great deal of experience and knowledge could be gained from a trial of a pair of these or even of a single one."[129]

Although the Enigma machine had been in existence for such a short period of time, the British and many other nations were already seeing its potential value. The Enigma was an engineering feat not only because of its complex encryption capabilities, but also because it was

[124] NA HW 25/6, Communication from *Enigma Chiffriermaschinen Aktiengesellschaft* about price and models available for order, Berlin, 2 June 1924.

[125] NA HW 25/6, Communication from J.H. Herring to Secretary of Air Ministry about Enigma Instruction Booklets, Berlin, 19 June 1924.

[126] *Ibid.*

[127] NA HW 25/6, Communication from Alistair Denniston to the Secretary of the Air Ministry, London, 1 July 1924.

[128] NA HW 25/6, Communication from Henry Tom to E.T.F Crowe, London, 31 January, 1925.

[129] NA HW 25/6, Report on Enigma machine from Government Code & Cypher School, London, 16 March 1926.

easy to operate. Although the initial model was quite heavy, future models would be made lighter and more compact so that it was portable. The portability would make it easy for possessors to issue it to frontline soldiers, air force squadrons, and the crews of naval vessels. The Enigma machine was beginning to revolutionize the field of cryptography at a time when governments ability to communicate secretly was increasingly important. The Germans were also beginning to take notice of this marvelous German invention as well.

Germany had motive enough to be interested in a device like the Enigma machine. Due to the limitations placed on Germany's military by the Versailles Treaty, the Enigma machine was an attractive piece of equipment.[130] The Enigma would allow the Germans to secretly coordinate the building of a military that exceeded the size limitations outlined in the Versailles treaty.[131] The German Post and War Departments first purchased the two available models in 1924 during the initial rush of purchases by many other countries.[132] The initial model, however, was not enough. The Germans immediately began to seek out ways to improve the Enigma machine. The German navy and army produced variations of the civilian Enigma in 1926 and 1928 respectively, and in 1930 a new military model was produced.[133] Soon thereafter the Enigma was used to send all communications within the German military.

In order to understand how British and Polish codebreakers broke the Enigma code, it is necessary to understand how the machine functioned. The Enigma was an electro-mechanical device that looked very similar to a typewriter. For the sake of this thesis, I will only describe the

---

[130] Wladyslaw Kozaczuk, *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two,* Ed. And Trans. By Christopher Kasparek, Ann Arbor, MI: University Publications of America, Inc., 1984, xiii.

[131] *Ibid.*

[132] NA HW 25/6, Communication from J.H. Herring to Secretary of Air Ministry about Enigma Instruction Booklets, Berlin, 19 June 1924.

[133] Kozaczuk, xiii; NA HW 25/16, Report written by S.A. Mayer, "The breaking up of the German Ciphering machine "ENIGMA" by the cryptological section in the 2nd Department of the General Staff of the Polish Armed Forces" London, 21 June 1977.

model used by the German military, and not the initial civilian model. The military model was made up of four basic parts: the keyboard, the plugboard, the rotors, and the lamp-board. The process of encoding began with the plugboard. The plugboard had twenty ports for twenty letters of the alphabet and had ten wires with a plug on either end. The operator would plug one of the wires into two letters, for example 'A' to 'B', the letters would then be switched. This meant that if the sender pressed 'B' it would initially be coded as 'A'.[134]

The next step in scrambling the message took place in the rotors. A sender needed three rotors to encrypt a message. Each of the rotors had twenty-six notches on it, one for every letter of the alphabet.[135] Inside the three rotors were hundreds of criss-crossed wires. Every time a sender pressed a key, the rotor on the right would rotate one notch, meaning that letter had been jumbled. Each time a letter on the keyboard was punched, the right rotor would turn and scramble the letter.[136] Even if the sender used the same letter twice in a row, that letter would be coded differently. For example, if the sender pressed the 'X' key twice, it might be coded as 'D' and 'Z'. Once the right rotor had made one complete cycle of twenty-six notches, it would turn the middle rotor over one notch. Once the middle rotor completed a full rotation, it would do the same to left rotor.[137]

Once a sender depressed a key and the letter was scrambled within the rotors the code was displayed on the lamp-board. The lamp-board was laid out exactly like the keyboard, with translucent discs that would be lit up by small light bulbs. So if the sender pressed 'W' that letter

[134] "The Enigma Machine: James Grime Demonstrates the Enigma Machine." The Enigma Project, http://enigma.maths.org/content/, (accessed 14 October 2013) . It should be noted that James Grime holds a Ph.D. in mathematics from Cambridge University and that this website is operated by Cambridge University in order to use the Enigma machine as an educational tool in secondary schools throughout the United Kingdom. In researching for this paper I found it incredibly difficult to comprehend the process of the Enigma encryption as it was described in books--no matter how hard many of the authors tried to simplify it--and so I found that this brief video tutorial gave the best possible explanation as to how the Enigma encrypted and decrypted messages.

[135] *Ibid.*

[136] *Ibid.*

[137] *Ibid.*

would be scrambled through the plugboard and the rotors and then appear as another letter, for example 'H', on the lamp-board.[138] Therefore 'H' was the letter 'W' was paired with on the plugboard. In order for someone receiving the message to decode it, they would have to set the rotors on their machine to the first position of the sender's rotors.[139] When the rotors were set to the sender's initial setting, the receiver would type in the coded message and the Enigma would decode it in plain text.

The complexity of the Enigma can be broken down in five ways, meaning that any code could be altered using five different variables. The first is the wiring of the discs.[140] The second variable was the the choice of disks. Standard German army Enigmas used five wheels and the Navy used eight.[141] The more wheels that were available for use the more options there were for scrambling the code. The third variable was the order of the disk settings.[142]The starting order of these three disks, if identified by anyone trying to break the code, would be crucial. By identifying the beginning setting, codebreakers could use this as basis for decryption. The fourth variable was the changing of disk rims, which meant that a disk could have any number of combinations of the order of the twenty-six letters numbers on it.[143] The final variable was the combinations between letters on the plugboard. All of these possible variables led to over one-hundred-billion possible combinations. The task for anyone, or any organization, to break the code would be monumental.

The British were not the only nation analyzing the Enigma machine with some level of scrutiny. Polish intelligence officials had been monitoring German radio traffic since the mid-

---

[138] *Ibid.*
[139] *Ibid.*
[140] Keegan, *Intelligence*, 175.
[141] *Ibid.*
[142] *Ibid.*
[143] *Ibid.*

twenties. In late January 1929 a Polish customs official seized an Enigma in Warsaw.[144] The Enigma had accidentally been mailed to Poland and the German Embassy official in Warsaw requested the package be sent back to Germany immediately.[145] The package, which had been intercepted on a Friday, was shipped back to Germany on the following Monday but not before two owners of a Warsaw communications company had examined it.[146] This was just the most recent chapter in what had become a vicious intelligence duel between Poland and Germany.

This clash was the result of the creation of Poland following the First World War. Since part of the newly formed Poland was made up of former German territory, the Poles were justifiably suspicious that the Germans were plotting to re-seize their old territory. By the end of the decade the Germans had begun using the Enigma for almost all radio communications. The Poles continued to try to break the code but were relying solely on mathematical process.[147] Even when provided with one of the commercial Enigmas the Polish code-breakers were unable to make much headway beyond having a basic grasp of how the machine worked mechanically. The Poles relied solely on intercepted radio transmissions in order to search for patterns in the code.[148] Without materials relating to the military Enigmas, then the Polish code-breakers were left groping in the dark.

The supporting materials became available three years later in November 1932. They were not handed over to the Poles but to the French. The materials were provided to the Deuxième Bureau by Hans Thilo Schmidt, a forty-three year old employee at the German Defense Ministry Cipher Office. Schmidt, who had access to secret Enigma cipher books, met

---

[144] Hugh Sebag-Montefiore, *Enigma: The Battle for the Code*, (Chichester, UK: John Wiley & Sons, Inc., 2000), 21.
[145] *Ibid.*, 21.
[146] *Ibid.*, 21.
[147] Kozaczuk, *Enigma*, 12.
[148] *Ibid*.

with Bureau agent Rodolphe Lemoine on 1 November at the Gran Hotel in Verviers, Belgium.[149] A week later they met again in Verviers. This time Lemoine brought along Gustav Bertrand, a code expert, to assess the value of the materials Schmidt brought from the cipher office. Schmidt had managed to bring the instruction manuals for the German army's version of the Enigma.[150] Lemoine paid Schmidt 10,000 marks for the manuals with the guarantee of further payment for any more materials Schmidt could produce. Bertrand photographed the codebooks and knew that Schmidt had the potential to single-handedly help the French break the code.

Over the next few years Schmidt, who had been given the codename "Asche", provided a wealth of information to the French. Included were various codes—type A, B, C, D, E—used by the German military, documents concerning machine ciphers and keying instructions, and the monthly table keys for the German army for the month of December 1931.[151] Schmidt's contributions were incredibly valuable, but he was unable to obtain any documents which explicitly described how the military Enigma functioned. By studying materials from previous months the Poles could begin to understand the structure of codes.

On returning to Deuxième Bureau headquarters in Paris, Bertrand was urged to seek the opinion of the British Secret Intelligence Service (SIS). Wilfred Dunderdale, head of the SIS French station, inspected Bertrand's photographs and reached the conclusion, along with Bertrand and other French codebreakers, that the manuals alone could not break the code.[152] The manuals gave the French a starting point. Bertrand was aware of the Polish code breaking efforts

[149] Sebag-Montefiore, *Enigma: The Battle for the Code*, 19.
[150] *Ibid.*
[151] Kozaczuk, *Enigma*, 17-18.
[152] Sebag-Montefiore, *Enigma: The Battle for the Code*, 20.

and requested permission to take copies of the photographs to Warsaw. Permission was granted and he left promptly.[153]

Ever since the interception of the Enigma by the customs officer, the Poles had been incredibly busy assembling the best codebreakers they could find. This task was difficult because not only was the field of cryptanalysis relatively new, but so was the Polish government. Mathematicians were heavily recruited for this purpose. Marian Rejewski, Henryk Zygalski, and Jerzy Rozycki formed the core of this group.[154] All three mathematicians had excelled in a cryptology course offered by two members of the Polish General Staff at PoznaDUniversity•s Mathematics Institute in January 1929.[155] In addition to academic aptitude, Rejewski, Zygalski, Rozycki and the other mathematicians recruited all spoke German fluently. Many of them had grown up in parts of the country formerly belonging to Germany.

When Bertrand arrived in Warsaw in December 1932 there had been no official correspondence between the Polish cryptologists and the French. An arrangement was made between Bertrand and Major Gwido Langer, the head of the Polish Cipher Bureau.[156] It was decided that France and Poland would divide the duties of cracking the Enigma. Poland would be in charge of trying to break the radio intercepts while France would continue to provide the Polish codebreakers with up-to-date intelligence.[157] Equipped with Schmidt's materials, Rejewski was able to ascertain a basic understanding of the Enigma's enciphering and deciphering functions. In order to break the code Rejewski knew that he must be able to replicate

[153] *Ibid*.
[154] Keegan, *Intelligence*, 177.
[155] Kozaczuk, *Enigma*, 1.
[156] *Ibid.*, 18.
[157] *Ibid.*

an Enigma.[158] He could not replicate an Enigma without first knowing the wheel settings for the device. As mentioned before, the position of the wheels determined how outgoing messages were encrypted and incoming messages were decrypted. During this time the Germans changed the wheel combination once a month and all machines used the same combination when sending or receiving messages.

With the help of the materials Schmidt had procured Rejewski and the Poles were able to replicate an operational Enigma of their own by January 1933.[159] By the following month the Polish Cipher Bureau had commissioned AVA Radio Manufacturing Company of Warsaw to construct fifteen replicas of the Enigma.[160] By constructing these Enigma replicas the Polish codebreakers were able to begin breaking encrypted German radio messages with moderate success. This success sprouted from the Polish ability to identify a German pattern in the traffic. At this time the Germans were sending the wheel setting twice at the beginning of each transmission.[161] The transmitted wheel setting was encrypted twice, but it still allowed the Polish codebreakers to find a pattern and with the help of their own Enigmas to crack the code. In addition to cracking the code, the Polish were aided further by discovering how the three cylinders were wired.[162] Once the Polish Cipher Bureau was able to replicate the wiring of the cylinders, they were able to program their fifteen replicas in the same way. This replication of cylinder wiring was one of the two breakthroughs accomplished by the Poles. It meant that the number of variables was drastically reduced. S.A. Meyer, the head of Polish Intelligence in the pre-war years, later concluded "By the end of 1937 our cryptologists mastered completely the

[158] Sebag-Montefiore, *Enigma: The Battle for the Code*, 37.
[159] Kozaczuk, *Enigma*, 25.
[160]*Ibid*.
[161] Sebag-Montefiore, *Enigma: The Battle for the Code*, 41.
[162] NA HW 25/16, Report written by S.A. Mayer, "The breaking up of the German Ciphering machine "ENIGMA" by the cryptological section in the 2nd Department of the General Staff of the Polish Armed Forces" London, 21 June 1977.

reading of the intercepted German radiograms ciphered by "Enigma.""[163] Meyer stated that as late as January 1938 the Polish cryptologists were breaking German codes with one-hundred percent accuracy.[164]

The Polish ability to read German messages with ease ended later that year. In September 1938 the Germans no longer sent the message key at the beginning of messages, thus ending the ability of the Polish codebreakers to decipher the transmissions.[165] The Germans also added two additional discs and more circuits to the plugboards of the Enigma, multiplying the number of possible combinations substantially.[166] The Polish codebreakers could no longer rely on finding patterns at the beginning of messages or wire their replica Enigmas accordingly, so they were forced to improvise. The Polish Cipher Bureau now had to rediscover the wiring of the discs. After years of success, they were starting anew.

The result was the creation of the *bomba*, a series of Enigmas wired together that were to identify the beginning wheel positions and wiring of Enigmas.[167] This was the first attempt to create an electromechanical device that could help alleviate the burden on the codebreakers. The code would continue to become more complex, and it would soon become impossible for humans alone to break it with mathematical reason and pattern identification. There became a need for a device that could lessen the amount of data for the codebreakers to sort through. The Poles also used perforated paper sheets to help them find patterns, a technique pioneered by Zygalski. The perforated sheets served as a means to catalogue repeated letters in transmissions. These repeated letters were called "females" and would allow the Poles to rule out up to forty

---

[163] *Ibid.*
[164] *Ibid.*
[165] Sebag-Montefiore, *Enigma: The Battle for the Code*, 41.
[166] Keegan, *Intelligence*, 180.
[167] Sebag-Montefiore, *Enigma: The Battle for the Code*, 326.

percent of possible other letters when found.[168] Whenever two females appeared in any transmission on a given day, a hole was punched in the perforated sheets and these cards could be used to pinpoint the starting position of the Enigma wheels.[169]

There was a problem with the perforated sheets. So many of the sheets were required that it was impossible to produce them in the needed numbers, largely because each sheet had to be cut by hand.[170]There was also a demand for even more Enigma machines. The Polish Cipher Bureau estimated that it would need sixty *bomba*, with each *bomba* comprised of six Enigmas.[171] Manufacturing more than three-hundred Enigmas would be incredibly expensive. The Polish codebreakers were gradually beginning to lose in their battle with the code. The Enigma was becoming increasingly more complex, and the *bomba* was unable to keep up.

As the troubles of the Polish Cipher Bureau mounted, the General Staff decided to expand their contact with allies. At the end of 1938, Gustav Bertrand organized a tri-lateral intelligence meeting among the Poles, French, and British in Paris.[172] The meeting took place from 7-9 January 1939. The Polish contingent was under orders to not divulge any of their breakthroughs to the British and French. Denniston, who was present at the meeting, wrote a report upon returning to London. He concluded that Polish knowledge regarding the new Enigma model was "nill" and that the Poles "declaimed a pamphlet which contained nothing new to us."[173] The British left Paris in January unimpressed and unaided. Polish struggles continued, and yet they remained silent. The age of progress, however, was over. As the period of

---

[168]*Ibid.*.

[169] Sebag-Montefiore, *Enigma: The Battle for the Code,*43.

[170] Kozaczuk, *Enigma*, 55.

[171]*Ibid.* .

[172] *Ibid.*, 57.

[173] NA 25/12, Report by A.G. Denniston on Meeting with Polish and French Codebreakers in Paris, 13 January 1939.

stagnation progressed, the Poles began to panic. They simply were no longer making strides against the code.

After the meeting in Paris the Poles continued their development of the *bomba*. They were able to achieve brief glimpses of success in the months before the beginning of the war in September. The Polish *bomba* managed to help break some messages sent by the Luftwaffe.[174] By the summer the Poles were unable to progress further. They were running out of time. Following German expansions into Austria and Czechoslovakia, the Poles were all too aware that they might be the next target for invasion. It became increasingly apparent to the Poles that they needed to pass along what knowledge of the Enigma they had before it was too late. They set up a second meeting in Warsaw for July 1939.

At the meeting in Warsaw the Poles revealed that they had broken the Enigma code.[175] Both the French and British were incensed by the fact they had been kept in the dark. Dilly Knox wrote a report on the meeting, stating that the Poles "had a good supply of mechanical gadgets" but were "understaffed."[176] Knox and the French delegation were shown into the Polish Cipher Bureau and given full disclosure about Polish breakthroughs. Knox later wrote that Polish methods tended to employ "electricity and some of them are neat."[177] One of these neat Polish devices was the *bomba*. Knox wrote "Precisely how the machine (Bombe) works I do not know; at present it is not yielding results."[178] The *bomba* impressed Knox, as British methods were still

[174] NA HW 25/16, Report written by S.A. Mayer, "The breaking up of the German Ciphering machine "ENIGMA" by the cryptological section in the 2nd Department of the General Staff of the Polish Armed Forces" London, 21 June 1977.
[175] Sebag-Montefiore, *Enigma: The Battle for the Code*, 45.
[176] NA 25/12, Report by D. Knox on Tri-Lateral Meeting in Warsaw, London, 4 August 1939.
[177] *Ibid.*
[178] *Ibid.*

done by hand. He referred to the British approach as "our humble method of charts."[179] Knox penned a quick letter to Denniston from the Hotel Bristol in Warsaw in which he expressed many of his opinions about the *bomba*. Knox began by writing "The Poles have just got the machine to Sept. 15th 38 out by luck."[180] The Poles had managed to break the codes from one day eight months prior to the meeting, but Knox was clearly not that impressed with the task or the methods. "They must have done very well to determine the two new wheels," Knox continued "How they did might be important. I have not deciphered this."[181] Once again, Knox seemed to be unconvinced and unconcerned with how the Poles achieved their progress.

Knox's letter to Denniston alludes to a rift between the British and Polish philosophies in dealing with the code, the foremost being that the Poles did not think there were any repetitions in German army messages, while Knox disagreed. The remainder of the meeting was, according to Knox, uneventful. Knox later wrote in a five page report about the meeting that "Almost all our guesses have been right."[182]The British did not leave with much information, but Knox did not pass on giving the Poles some credit. He wrote, "I think we may hand some bouquets to the Poles for their lucky shot, but far more for their surmounting the difficulties after 15 September if only for two months."[183] The difficulties Knox refers to were the changing in German transmission protocol and the addition of more Enigma wheels to the machines. The Poles had not been able to keep up with the changes for very long. Knox acknowledged that although the British and the Poles disagreed on some of the fundamental approaches of breaking the code, the Poles had achieved some brief successes and that was notable.

---

[179] *Ibid.*

[180] NA HW 25/12, Letter from Knox to Denniston about Tri-Lateral Meetings in Warsaw, London, July 1939.

[181] *Ibid.*

[182] NA HW 25/12, Report by D. Knox on Tri-Lateral Meeting in Warsaw, London, 4 August 1939

[183] *Ibid.*

At the conclusion of the Warsaw meeting, both Britain and France were given a replica of the Enigma machine by the Poles.[184] For the most part the meeting had marginal results. Many of their methods were unreliable and outdated, according to Knox, and the British and Poles disagreed on the fundamental approach to cracking the code. Knox wrote “A serious difficulty of liaison is that their notation differs entirely from ours since we use numbers where they use letters and vice versa.”[185] The revealing of the *bomba* remained the one silver lining of the meeting. Even still, the device was not functioning and would later have to be built anew by Alan Turing and Gordon Welchman. The Polish *bomba* became the kernel from which the British would seek something useful.

On 1 September German forces surged over the Polish border. Four days following the invasion the Polish codebreakers were evacuated to Warsaw.[186] From there they moved towards the Romanian border by train. The journey was deterred by German air raids and widespread damage to the railway. On 17 September Rejewski, Zygalski, and Rozycki all crossed the Romanian border and began their journey towards Bucharest. They tried to contact the British embassy upon arrival, but after several hours of waiting they turned to the French.[187] After the French bribed the customs officers and produced false passports and travel orders, the three Polish codebreakers left Romania and arrived in southern France by the end of the month.[188]

Upon arriving in France Lieutenant Colonel Langer was invited by the French to join their codebreaking section. Langer would be allowed to work with his previous staff. Langer sought approval from the Polish government-in-exile and it was granted. On 20 October 1940

[184] Sebag-Montefiore, *Enigma: The Battle for the Code,* 45.
[185] NA 25/12, Report by D. Knox on Tri-Lateral Meeting in Warsaw, London, 4 August 1939
[186] Kozaczuk, *Enigma,* 70.
[187] *Ibid.,* 74.
[188] *Ibid.,* 75.

Langer arrived at P.C. Bruno, a French codebreaking base located at Castle Vignolles thirty-five kilometers southeast of Paris.[189] Langer, Rejewski, Zygalski, Rozycki, and ten other Polish staff who had managed to escape the German invasion joined a group of both French and British codebreakers. According to Langer's papers, he was not impressed by the operation at P.C. Bruno. The French did not find it necessary to study the Enigma machine that the Poles had given them.[190] Langer was impressed, however, when he visited London and learned that the British had already allocated £12,000 to the reproduction of the Enigma supplied to them by the Poles. There was also the recurring issue of the perforated sheets, which had to be produced in Britain.

The Poles would be at P.C. Bruno for approximately seven months. During that time they were able to make some progress against the German code. Between 20 October 1939 and 23 June 1940 the codebreakers at P.C. Bruno read 8,440 total messages. Of these messages 1,151 pertained to the German invasion of Norway, 5,084 messages were about the campaign in France, 1,085 were about matters in "the Russian sector", 833 messages were concerned with various other areas, and the remaining 287 were about clandestine German radio stations.[191] The British played an integral part in the breaking of codes at P.C. Bruno. Between the work done in Britain and the codebreakers on site in France, the British accounted for 83% of key breaks.[192] The division of labor between P.C. Bruno and Britain was one reason the Allies were able to accomplish what breaks they could. The fact remained, however, that P.C. Bruno lacked the

[189] NA HW 25/16, Report written by S.A. Mayer, "The breaking up of the German Ciphering machine "ENIGMA" by the cryptological section in the 2nd Department of the General Staff of the Polish Armed Forces" based on the personal papers of Gwido Langer, London, 21 June 1977.

[190] *Ibid.*

[191] NA HW 25/16, Report written by S.A. Mayer, "The breaking up of the German Ciphering machine "ENIGMA" by the cryptological section in the 2nd Department of the General Staff of the Polish Armed Forces" based on the personal papers of Gwido Langer, London, 21 June 1977.

[192] *Ibid.*

technical facilities to properly intercept and analyze German ciphers.[193] P.C. Bruno was only a temporary fix for the mounting Enigma problem.

The progress made during the seven months in France was minimal. Messages had been read, but not with any regularity. All told the allied codebreakers only managed to break the daily keys for a total of two days out of the seven months.[194] Without the daily key the British, French, and Poles were not able to consistently read codes. Out of the thousands of messages sent every day the codebreakers at P.C. Bruno were reading an average of thirty-three. It was simply not enough.

After 24 June 1940 P.C. Bruno ceased to exist.[195] The German invasion of France put the Polish codebreakers to flight once again. They were flown to Oran and then to Algiers.[196] Langer tried to be evacuated with Polish soldier to Britain, but was unable to. He later received permission from the Polish Government in exile—now headquartered in London—to work with French codebreaking stations in North Africa. The principal Polish codebreakers—Langer, Rejewski, Zygalski, Rozycki—were all initially present in North Africa. One by one they broke apart. Rozycki later drowned in January 1942 following the sinking of a French ship in the Mediterranean Sea.[197] Rejewski spent part of the war in a Spanish prison later returned to Poland.[198] He remained disillusioned about his cryptology work, this may have been the result of the death of his eleven year old son in 1947, or the fact that Rejweski was still recovering from

[193] *Ibid.*
[194] *Ibid.*
[195] *Ibid.*
[196] *Ibid.*
[197] NA HW 25/16, Report written by S.A. Mayer, "The breaking up of the German Ciphering machine "ENIGMA" by the cryptological section in the 2nd Department of the General Staff of the Polish Armed Forces" based on the personal papers of Gwido Langer, London, 21 June 1977.
[198] *Ibid.*

rheumatism. Whatever the specific reason, Rejewski's war experience was traumatic and he seemed to be incapable of returning for much of the post-war period. Colonel Langer managed to find his way to London in mid-1945 and died three years later.[199] Zygalski, the man responsible for the creation of the punch card system, was the only one of the Polish codebreakers who made it Britain in time to work at Bletchley Park. The Poles had certainly made incredible strides against the Enigma code. Following the German invasion of France the Polish codebreakers contribution to breaking the code ended. Sole responsibility for analysis and breaking of the code now fell on the shoulders of the British.

In the few years leading up to the outbreak of the Second World War, the British had been making improvements to Government Code & Cypher School (GC&CS). Following the First World War Room 40 had been renamed GC&CS and had been brought under the auspices of MI-6.[200] The immediate function of GC&CS post-war era was monitoring signals intelligence originating from the newly established Soviet Union. Knox and Denniston had helped prove the worth of signals intelligence and GC&CS now became a permanent department in London. GC&CS remained a small division until early 1939. Politicians and military leaders in London became concerned about having many of their vital offices located in the center of the capital. In order to avoid the widespread destruction, many of these departments began to relocate outside of London.[201]

Government Code & Cypher School found a new home in Milton Keynes, Buckinghamshire located fifty miles north of London. The new headquarters for British codebreaking was now located in a Victorian mansion nestled on a well-manicured country

[199] *Ibid.*
[200] Keith Jeffrey, *The Secret History of MI6*, (New York: Penguin, 2010), 209-211.
[201] Jeffrey, *The Secret History of MI6*, 319.

estate. The estate was called Bletchley Park. The days of cramped offices in Room 40 of the admiralty building and Dilly Knox's long baths down the hall were no more. This location was chosen not only because it was away from London, but also because its isolation made it easy to secure. For many years following the Second World War the wartime role of Bletchley Park remained a closely guarded national secret. The final reason for relocating GC&CS was for recruiting purposes. Bletchley Park was located half-way between Oxford and Cambridge.[202] This location allowed Denniston and Knox the luxury of recruiting personnel from Britain's flagship universities.

After relocating to Bletchley Park, A.G. Denniston began to focus on the expansion of personnel and staff. In a memo addressed to the foreign office on 22 April 1939 Denniston briefly described what kind of personnel he wanted at GC&CS. He wrote "As the matter is urgent we prefer to find a man of 40-50 with linguistic qualities and, in this case, a commercial training. We can rapidly give him the necessary technical training in cipher work and if he shows no aptitude we do not keep him."[203] Denniston outlined their immediate needs: linguistic expertise was primary, technical knowledge could be learned. Linguistics was one of the necessary foundations for any codebreaker. These traits had served Britain well in the First World War, when most codes had been broken by linguists isolating patterns. Denniston summed up his thoughts later in the memo, writing "Second-class brains willing to take a second-class job are no good to us – it is waste of money and energy."[204] For the next few years Denniston would continue to seek out first class minds to work at Bletchley Park.

---

[202] *Ibid.*
[203] NA HW 72/1, Letter from A.G. Denniston to Quarmby at the Foreign Office, London, 22 April 1939.
[204] *Ibid.*

Dozens of brilliant men and women would devote years to the study and breaking of the Enigma code. Not all of the codebreakers were recruited directly from universities. For instance, senior members of the British chess team were targeted for GC&CS at the outbreak of the war.[205] Two of these team members, Stuart Milner-Barry and Conel Hugh O'Donel Alexander both had impeccable academic credentials. Milner-Barry had been a contemporary of Denniston's at Trinity College, Cambridge and Alexander had earned a First in Mathematics at King's College, Cambridge.[206] Another codebreaker was selected by their ability to solve the *Daily Telegraph* crossword puzzle in less than twelve minutes.[207] There was one particularly brilliant man, however, that would become the poster child for the Bletchley park code breaker.

Alan M. Turing was exceptionally intelligent, even when compared to his contemporaries at Bletchley Park. Turing was a twenty-eight year old mathematical genius who had just finished his PhD dissertation at Princeton University when he was first contacted by CG&CS in 1938.[208] Turing had been fascinated by codes and ciphers for a number of years. It is quite possible that he would have spoken about them amidst his fellow dons and peers at King's College, Cambridge.[209] He arrived at Bletchley Park on 4 September 1939, just one day after Britain had declared war on Germany.[210] Turing's arrival at Bletchley Park was critical for one major reason: he would immediately seek to develop a mechanical approach to cracking the code. Turing was one of dozens of academics at Bletchley, and he was soon assigned to Hut 8, the center assigned

---

[205] Ronald Lewin, *Ultra Goes to War: The First Account of World War II's Greatest Secret Based on Official Documents,* (New York: McGraw Hill, 1978).

[206] *Ibid.*

[207] Sinclair McKay, *The Secret Lives of the Codebreakers: The Men and Women Who Cracked the Enigma Code at Bletchley Park,* (London: Penguin, 2010), 18-19.

[208] Andrew Hodges, *Alan Turing: The Enigma* (New York, NY: Simon and Schuster, 1983)., 148.

[209] *Ibid.,* 149

[210] *Ibid.,* 160.

the task of breaking the German naval code.[211] He joined a team that was made up of Knox, Gordon Welchman, Peter Twinn, and John Jeffreys.[212] Turing immediately turned his attention towards two objectives: breaking the Naval Enigma and developing a mechanism that could break the daily Enigma keys.[213]

The presence of Alan Turing at Bletchley Park represents a rare synthesis between personal ambition and strategic mission. While at Princeton Turing had authored a paper entitled "On Computable Numbers, With an Application to the *Entscheidungsproblem*."[214] In this article Turing laid down the mathematical foundation for a basic computing machine. This interest was encouraged and cultivated by Turing's dissertation advisor, Alonzo Church. Together they authored the Turing-Church thesis, which sought to define which mathematical problems were solvable by the formal arithmetical process and those that could not be solved.[215] The Turing-Church thesis proved that the *Entscheidungsproblem* (decision problem) and several other mathematical problems were, in fact, unsolvable by human logic.[216] This gap in human knowledge prompted the design of the Turing computer, a device that would help solve the aforementioned unsolvable problems. The device was never built, but Turing had experience designing primitive computers as he arrived at Bletchley Park.

Turing's research background fit perfectly with the needs of GC&CS. In order for the British to crack the code they would need to create an electromechanical device to process vast amounts of information, sort through the data, and isolate patterns within the data. The Polish

---

[211] Welchman, *The Hut Six Story,* 33.

[212] Frode Weierud, "Prof's Book: Seen in the Light of Cryptologic History," in *Alan Turing: His Work and Impact*. Ed. by S. Barry Cooper and Jan van Leeuwen, (Walden, MA: Elsevier Science, 2013), 413-16.

[213] *Ibid*., 415.

[214] "Alan Turing," *Encyclopedia Britannica*, http://www.britannica.com/EBchecked/topic/609739/Alan-Turing, (accessed 21 August 2014).

[215] *Ibid.*

[216] *Ibid.*

codebreakers had managed to construct a device—the *bomba*—that could perform basic functions in this vein, but it had not been able to keep up with the developments and changes in the Enigma code. The new computing device would have to be an exceptional piece of engineering.

In many ways the codebreakers at GC&CS picked up where their predecessors at Room 40 had left off in 1918. They had recruited the keenest minds from Oxford, Cambridge, and other sources. They had the intellectual raw materials in place, but now needed to gather up-to-date intelligence, and develop a new mechanical aide in combating the code. They had consulted the Poles, analyzed their methods, and decided to begin anew without Polish assistance.

Alan Turing and the new codebreakers at Bletchley Park would have to take the basic solutions the Poles had pioneered and improve on them substantially in order to properly attack the code. To make matters worse, Britain was now completely isolated in the fight against Germany. In many ways the plight of the codebreakers was representative of the strategic situation: Britain against the code, and Britain against Germany. From September 1939 forwards the pressure against Britain and the codebreakers was gradually mounting. From that point on every day, hour, and second was crucial in solving the code and possibly saving a nation.

CHAPTER FOUR

THE BLETCHLEY PARK CIRCUS: TURING, WELCHMAN, THE CREATION OF THE BOMBE, AND BREAKING OF THE GERMAN NAVAL CODE, 1940-43

> "The king hath note of all that they intend, by interception which they dream not of."
>
> —William Shakespeare, *Henry V*

After Turing's arrival at Bletchley Park, the commanders at GC&CS began to concentrate their efforts on finding a mechanical solution to cracking the German code. In essence, the British wanted to create an improved version of the Polish *bomba*. Even though the Polish codebreakers were working at P.C. Bruno and were receiving aid from the British, Knox and Denniston wanted GC&CS to operate as independently and effectively as possible. The time for serious collaboration had, ironically, began and ended after the tri-lateral discussions in July. The British helped the French and Poles, but their efforts were concentrated primarily at Bletchley Park. Codebreaking was tri-lateral in appearance only. The previous chapters of this thesis have outlined the establishment of the British codebreaking service and the pre-war work of the Poles on the Enigma code. This chapter will focus on how the British managed to solve and break the Enigma code consistently. The sustained British success stemmed from two major differences with the Poles. The financial backing the British received allowed them to have a larger codebreaking staff and the ability to produce more bombes. The British were also able to eventually capture up-to-date Enigma codebooks and materials. These factors were the major factors that drove the British codebreaking mission to a period of sustained success in three years.

There were three major codes used by the German military: an army, air force, and naval code. I will focus mostly on the naval code, which was the most complicated and took the longest to break. But I will also explain how GC&CS aided in both the Battle of Britain and the monitoring of Operation Sea Lion by cracking German army and air force codes. The Poles had made an important contribution to the overall mission, but their methods had failed. The British now had to adopt their own methods in order to crack the code. The methods began without many parameters, but the objective of the British codebreakers at Bletchley Park was simple: break the code faster and more efficiently. Throughout the time period 1940-43 the British would be challenged by the clock. Every day the code was changed. A new challenge presented itself with the passing of every twenty-four hours.

Alan Turing's arrival at Bletchley Park was important, but he was not the only codebreaker who would play an intricate role in the development of the British response to Enigma. Gordon Welchman would become one of the only Bletchley Park codebreakers, along with Turing, who would enjoy a level of celebrity and public exposure when their exploits were first written about publicly in the 1970s. Welchman's background in mathematics was similar to Turing's. Welchman studied at Trinity College, Cambridge and scored exceptionally well in the Tripos, the vigorous series of examinations undertaken throughout an undergraduate career.[217] He returned to Cambridge a year following graduation and became a fellow at Sidney Sussex College. Welchman was a popular faculty member, was known for his excellent tuba playing and the inability to light his pipe while lecturing.[218] Like Turing, Welchman was approached by GC&CS in 1938, when he was asked if in the case of war he would provide his expertise for King and Country. On 4 September 1939 Welchman arrived at Bletchley Park and was assigned

[217] Joel Greenburg, *Gordon Welchman: Bletchley Park's Architect of Ultra Intellige*nce, (New York: Frontline Books, 2014), 32.

[218] *Ibid.*

to Hut 6 in order to help break the air force code.[219] His influence would reach beyond Together both of these men would be the greatest influence in the breaking the code.

When Turing arrived at Bletchley Park in September 1939 he threw himself into the task of breaking the naval code. Turing viewed the naval code as the ultimate challenge, primarily because it was the most difficult code to decipher. In addition to this, progress was already being made on the army and air force codes.[220] Turing was later quoted as saying he sought out the naval code "because no one else was doing anything about it and I could have it to myself."[221] He had to start somewhere, however. Turing immediately studied where the Poles had begun to fail: May 1937.[222] It was during this time that the Germans were no longer sending the decryption key at the beginning and end of every message. It was this change in transmission policy that had befuddled the Poles so profoundly. Turing began analyze the back-dated messages in hopes of finding a new solution.

Turing has received a tremendous amount of attention for his work at Bletchley Park. It should be stated that he was, by no means, popular with his peers initially. It is important that one understands Turing's eccentricities and personality, in order to comprehend the mindset and character of the codebreakers at Bletchley Park. Although Turing's behavior was not indicative of the entire staff at GC&CS, he serves as a prime example for many of the personality types housed there. Turing reveled in isolation, a trait reflected in his sport of choice, long-distance running. This desire for remoteness was partially motivated by his social personality, or lack thereof. He regularly avoided chit-chat, or much form of conversation at all.[223] Turing's dislike

---

[219] *Ibid.*
[220] HW 25/2, "The History of Hut Eight, 1939-45" written by A.P. Mahon, London, July 1945.
[221] *Ibid.*
[222] *Ibid.*
[223] Serbag-Montifore, *Enigma: Battle for the Code*, 96-97.

for talk was so profound that he would walk with his head down when he went to the canteen for lunch. Should someone attempt to speak to him, Turing would beat a hasty retreat to avoid them.[224] When Turing was dragged—we can assume unwillingly—into conversation he never made jokes, and never did more than smile when someone else made one.[225]

This eccentric behavior was heightened in summer. Turing suffered from hay fever, but would continue to bicycle through the countryside when the pollen count was high. In order to combat the pollen, he wore a gas mask.[226] The chain on his bicycle was faulty, but instead of fixing it he would count the rotations until the chain nearly slipped off, and then pedal backward to right the chain. The faulty bike also served another purpose: no one would steal it.[227] Turing took more aggressive precautions with his tea mug, however, and chained it to a radiator in the Cottage with a padlock. Turing's awkwardness was also intellectually driven. He loathed the prospect of working with anyone who he deemed to be less intelligent than himself. This initially presented a problem. Progress at Bletchley Park quickly became dependent on highly intelligent people working in close-quarters and with one another. Many of the individuals who worked at Bletchley Park would later be characterized as geniuses, but Turing and a few of his contemporaries achieved a higher rank, even amongst the hundreds of highly-gifted GC&CS staffers. Alan Turing became one of the significant driving forces within the cloistered and secret community of Bletchley Park.

Turing knew that in order to effectively handle the amount of Enigma transmissions, the process could not be done strictly by hand, which is the method employed successfully by the Poles until September 1938. This process would be too time-consuming. Turing was the first

[224] *Ibid.*
[225] *Ibid.*
[226] *Ibid*, 98.
[227] *Ibid.*

person to strongly advocate for the creation of a computing device that could handle the massive amounts of information, for it to shoulder the majority of the mathematical burden. Turing began his analysis of the code not in order to find a solution for humans, but for a machine. Therefore it was necessary for him to find a basic pattern in the new code. Turing's approach differed drastically from the Polish one because he was looking for a mechanical solution from the outside. In this way, the Polish failure benefited the British. The successful Polish approach, which was done exclusively by hand, had only been effective until September 1938. It was only then that the Polish had began to seriously engineer a mechanical approach. Thusly, the Polish *bomba* was only able to be successful in isolated incidents. Turing had the advantage of skipping this first step and picking-up where the Poles had left off.

The British and Turing did seek advice from direct communication with the Polish codebreakers. In early 1940 Turing travelled to France in order to discuss the code with the Poles at PC Bruno.[228] These meetings, however, were of no particular help to either side. Turing did not divulge that the British were building a newly improved bombe, or that they were devoting the bulk of their codebreaking manpower and financial resources to the operation at Bletchley Park. It seems as though the British were repaying their Polish allies for the silence of 1931-39. The silence between the two parties is profound. These meetings may seem important on the surface, but the fact that no information was exchanged says otherwise. The British had learned all they needed or wanted to know from the Poles in July. Further input, it seemed, was no longer necessary or desired.

[228] Kozaczuk, 97.

In early 1940 Turing outlined his philosophy about how the machine should be broken in a 152 page document called "the Prof's book."[229] "To understand the working of the machine," wrote Turing "it is best to separate [it] in our minds: the electric circuit of the machine without wheels, the circuit through the wheels, the mechanism for turning the wheels and for describing the positions of the wheels."[230] Throughout the Prof's book Turing explained how the code could be broken in larger and larger increments. Turing noted that small coded messages can be solved by hand and by using methods of deduction and analyzing patters in the text. This is the method that had been mastered by the Poles during the thirties. As the code becomes more complex, as it did in the latter part of the decade, it became necessary for the codebreaker to adapt more thorough methods. Turing used the Prof's book as a venue to describe his vision for codebreaking at Bletchley: the bombe, a mechanical device that could greatly eliminate the possible number of variables that had to be analyzed by the staff at GC&CS.

The bombe that Turing envisioned was designed to be an electro-mechanical device that could assist the codebreakers in determining the daily order of the Enigma rotors and the plugboard configuration for that given day.[231] After finding the position of the rotors—from left to right—the codebreakers could work out the rest of the variables themselves. In essence, the Turing bombe would drastically reduce the number of variables the codebreakers would need to analyze in order to figure out the daily Enigma key.[232] The Turing bombe would reduce these by running three letter pairs through its system at a high rate of speed.[233] By running through

[229] "Treatise on the Enigma, by A.M. Turing", Alan Turing Catalogue http://www.alanturing.net/turing_archive/archive/b/B05/B05-001.html (accessed 19 December 2014).
[230] *Ibid.*
[231] Keegan, *Intelligence in War*, 183.
[232] Sebag-Montifore, *Enigma: The Battle for the Code*, 329.
[233] Cooper and J. van Leeuwen. *Alan Turing: His Work and Impact*, 426.

possible Enigma key combinations it could determine which possible combinations were useful or not. This system became known as the “crib” system.[234]

The crib system depended on finding letter loops within the cribs themselves.[235] Letter loops occurred when “letters enciphered from one to another at different places in the crib.”[236] The interconnectedness of letter loops within cribs was another avenue by which the codebreakers could find patterns within the transmitted texts. Turing turned the letter loops theory into a foundation to design his bombe.[237] If the bombe could bring down the number of variables down to a manageable level than the codebreakers could use other methods—such as identifying letter loops—to break the code.

The Turing bombe would eliminate the possible rotor and plugboard connections that were *not* possible on any given day.[238] The bombe was able to do this by making a number of assumptions, the same assumptions made by the codebreakers themselves. This was achieved by wiring a number of Enigmas together without plugboards.[239] The wheels of these Enigmas were set to the assumed “crib” setting. The bombe ran all the possibilities for that particular crib, and if they produced nothing plausible, had their rotors adjusted one place.[240] The bombe would then run through all possible 17, 576 wheel settings and leave the codebreakers with a small number to test manually. The figure 17,576 was not completely representative of the massive odds the codebreakers faced. When the different plugboard, wheel settings, and wheel choices were

---

[234] Keegan, *Intelligence in War,* 184. Keegan makes the point that the term ‘crib’ originated in English public school Latin and Greek classes. A student would make a ‘crib sheet’ in order to cheat on an exam in one of the given languages.

[235] Tony Sale, “Alan Turing, the Enigma and the Bombe,” in *Alan Turing: His Work and Impact*. Ed. by S. Barry Cooper and Jan van Leeuwen, (Walden, MA: Elsevier Science, 2013), 426-432.

[236] *Ibid.,* 427.

[237] *Ibid*.

[238] Sebag-Montifore, *Enigma: The Battle for the Code*, 329.

[239] *Ibid,* 333.

[240] *Ibid.,*333.

factored in, there were 158,900,000,000,000 different combinations to account for.[241] The bombe would help them cut the number of combinations significantly and give the men at Bletchley Park a fighting chance, mathematically speaking.

The Turing bombes were built in early 1940 by a team at the British Tabulating Machinery (BTM) factory under the supervision of Harold Keen.[242] The engineers had to adapt from their peacetime manufacturing constraints. Before the war BTM had produced calculators and sorters only capable of carrying out single functions.[243] The bombe would need to be able to recognize consistent positions in the code where patterns appeared. Turing oversaw this construction, utilizing his pre-war study of computing machines, but much of the hands-on engineering work at BTM was supervised by Keen.[244] It was Keen's idea to use circular drums on the bombe so that they would replicate the wheels on the Enigma.[245] But instead of organizing the drums horizontally—as the wheels were on the Engima—Keen stacked the drums vertically. This way the drums were easily accessible to be changed. The drums were organized by eight colors: red, purple, green, yellow, brown, blue, black, and grey.[246] There were eight drums total, so each drum represented a possible wheel on the Enigma. Each drum had twenty-six letters and notches on it. The bombe was supposed to run all possible combination of letters in a given code. How did it know where to begin? It began with a guess, a "crib." This was Turing's idea. The first bombes could run through all possible combinations in a three-letter crib in twenty-two minutes.[247] This initially meant that the bombe could run through all possible three-letter combinations in twenty-two hours. The German army and air force were the only

[241] Greenberg, *Gordon Welchman*, 61.
[242] Hodges, *Alan Turing: The Enigma*, 181.
[243]*Ibid.*.
[244] Joel Greenberg, *Gordon Welchman*, 59.
[245] *Ibid.*
[246] *Ibid.*
[247] *Ibid.*

members of the service that used three cylinders. The German navy began using four cylinders, and had eight different cylinders to draw from, which made the number of significant combinations decidedly greater. The British thus needed to find a method for decreasing the amount of time it would take for the bombe to run through these solutions.

The first British bombe was delivered to Bletchley Park in March 1940.[248] The delivery of the machine only trumpeted the beginning of a new period of problem-solving for the codebreakers. It would take the codebreakers six months before they were able use the bombe effectively against any German code. Welchman biographer Joel Greenberg states, "A bombe did not magically tell BP's [Bletchley Park] cryptanalysts how the Enigma operators on a German communication network were setting up their machines."[249] The bombe was not an instant solution, but only the beginning of a protracted one.

At first, the arrival of the bombe only led to further confusion and uncertainty. The device was once compared to "the traditional German soldier, highly efficient but totally unintelligent; it could spot the perfectly correct answer but would ignore an immensely promising position involving one contradiction."[250] Turing seemed to be one of the only people who believed wholeheartedly in the power of the bombe, even though it was a long way from perfection. The physical construction of the machine was the first step, but programming the bombes correctly was the next challenge. This task would consume much of 1940. Turing would throw himself obsessively into the mission of perfecting his initial design. Hut 8 became the center of his mission. A.P. Mahon later recalled that "1940 was clearly a very trying period for

---

[248] Hodges, *Alan Turing: The Enigma*, 191.
[249] Greenberg, *Gordon Welchman*, 61.
[250] 25/2, "The History of Hut Eight, 1939-45" written by A.P. Mahon, London, July 1945

those outside 8."[251] As Mahon noted, "Unfortunately the bombe was an expensive apparatus and it was far from certain that it would work, or even if the bombe itself worked, that it would enable us to break enigma."[252] Any trust and confidence in the bombe was only worsened by the shroud of secrecy surrounding it, even within the confines of Bletchley Park.

Because the bombes were only being worked on in Hut 8, most of the remaining codebreakers were left effectively in the dark. Turing and fellow codebreaker, Peter Twinn, worked tirelessly on the code. Mahon later wrote the following critique of the two: "Turing and Twinn are brilliant, but like many brilliant people, they are not practical. They are untidy, they lose things, they can't copy out right, and they dither between theory and cribbing. Nor have they the determination of practical men."[253] For more than a year after the beginning of the war, Turing and his associates were being stretched to their intellectual capacities.

The key problem with Turing's cribbing method was that only certain cribs worked when plugged into the bombe.[254] As Mahon states, the sheer brilliance of Turing and other codebreakers was simply not enough. Sloppiness and inconsistency stood no chance against a code that had been broken only sporadically and by luck since September 1938. Sinclair McKay further elaborated on this point, writing that "It is broadly assumed nowadays that work at Bletchley required its inmates to be near-autistic, socially inept geniuses."[255] This was not true. The raw intellectual talent represented by Turing, Twinn, Denniston, and others had to be channeled and disciplined if it were to work against the Enigma.

[251] *Ibid.*
[252] *Ibid.*
[253] *Ibid.*
[254] *Ibid.*
[255] McKay, *The Secret Lives of Codebreakers*, 19.

As more time elapsed and progress remained limited, several outlandish ideas began circulating through Bletchley Park and Whitehall. The central theme behind many of these theories was how to obtain a copy of the daily Enigma key. How might this be accomplished? There were a variety of answers to this quandary, many of which were analyzed by Lieutenant Commander Ian Fleming, the man who would later become famous by creating fictional superspy James Bond. The first idea, proposed to Fleming by Knox and Frank Birch, was to try and solicit the daily key from the Germans by sending a bogus radio message.[256] Fleming thought the idea had some promise, and even had a few messages drawn up just in case. This plan had several drawbacks, however. The British did not know what code to transmit the message in, what radio frequency to send it on, what time of the day send it, and from what geographic position to send the message.[257] These questions were never answered and this plan was never put into action.

The false message plan was not the most bizarre of the alternatives proposed. Birch came up with another idea for obtaining Enigma materials. He wrote a memo to the Director of Naval Intelligence, in which he outlined this newest scheme. The plan would require an air-worthy German bomber from the Air Ministry and the selection of a "tough crew of five" that could fly the German plane and purposefully crash it into the English Channel.[258] Before crashing the plane, the crew—which would include a radio operator and fluent German speaker—would send a distress message.[259] Once the crew of the plane was picked up by a German rescue vessel, the disguised British would kill the German crew and pilot the craft back to a British port. Once the craft was captured British would be able to access its naval codebook and utilize it. This plan

[256] HW 25/2, "The History of Hut Eight, 1939-45" written by A.P. Mahon, London, July 1945.
[257] *Ibid*.
[258] *Ibid.*
[259] *Ibid.*

received some traction and was codenamed Operation Ruthless. As Mahon recounted, this "somewhat ungentlemanly scheme" never came to fruition. Several detailed plans were drawn up, but Operation Ruthless would never be enacted.

What is the significance of these plans if they were never used? The planning of these operations illustrates two things. Firstly, the lack of confidence Knox and other high-ranking Bletchley Park commanders had in the men assigned to Hut 8. The strain of breaking the code and lack of progress resulted in senior members of Bletchley Park having to dream up these fantastic operations. Almost anything, no matter how improbable and unlikely, that could give the British a better chance of breaking the naval code was considered. The fact that Knox and Birch thought that strategically crashing a plane into the English Channel could yield better results is alarming. When one considers how precarious crashing a plane into water could be—whether purposefully or not—it does make one wonder how much faith there was in the development of the bombe. Secondly, these schemes reveal the desperate need for the British to capture up-to-date Enigma materials. The progress the supervisors at Bletchley Park needed would come soon, and not from Turing, but from Gordon Welchman.

At the beginning of the war Gordon Welchman was assigned to study patterns in Enigma traffic and transmissions, and have nothing to do with the bombe. It was during this time that he would experience two dramatic breakthroughs relating to indicator settings and Enigma indicator messages. In his account of his war-time work Welchman later recalled:

> "People have asked how these breakthroughs came to me, and it is really very hard to explain. Basically the answer goes back to a memory from childhood; that of being lucky enough, with no purposeful effort on my part, to find myself opposite the vacant chair when the music stopped."[260]

[260] Welchman, *The Hut Six Story*, 59.

Welchman may have later described these breakthroughs as chance, but they cannot be understated. It is quite possible that without Welchman's chance breakthroughs than the British would not have made progress as quickly as they did.

It was while working in virtual isolation that Welchman developed a ten step approach to cracking the code. Isolation is not an understatement. Welchman was working in a small building, Elmer's School, located behind the Bletchley Park mansion.[261] Everything about Bletchley Park was highly compartmentalized, and it was only because of Welchman's natural curiosity that he began to conceive of this idea. The process he devised targeted to reveal the three letter indicator setting. The first three steps focused on the isolation of two three letter pairs in code that were repeated in the preliminary part of transmissions.[262] Once Welchman had calculated the probability of these three-letter pairs repeating in a given message on a given day, this provided him with a manageable number of combinations. Step five required Welchman to ignore the possible plugboard settings and focus instead on the sixty possible wheel orders and 17,576 wheel positions, which meant he was dealing with only a million combinations as opposed to two hundred trillion.[263] Steps six and seven focused on further calculation of probabilities and the study of perforated sheets to eliminate further possibilities.[264] The final two steps were completed by careful analysis of the perforated sheets that would result in the similarities.[265] This method represented the initial process that the British used. It focused on finding a consistent "probable word" that would appear consistently in messages.[266] Given the

[261] *Ibid.*, 34-37.
[262] Keegan, *Intelligence in War,* 181.
[263] Welchman, *The Hut Six Story,* 71.
[264] Keegan, *Intelligence in War,* 182.
[265] *Ibid.*
[266] Hodges, *Alan Turing: The Enigma,* 179

repetitive nature of certain parts of transmissions, this technique did possess credence but would rely on the messages being analyzed by hand.

Welchman was very pleased with this nine-step process. Once it was completed he quickly dashed over to tell Knox about it. Knox was not pleased. The system that Welchman devised was already being worked on by John Jeffreys.[267] In addition to this, the Poles had already tried this method with the Zygalski sheets. Knox had been told this at the meeting in Warsaw some months prior. Knox did not, however, let many other people know this. Such a miscommunication seems like an oversight, but one must consider several factors. The first was that Bletchley Park was an incredibly chaotic place in October 1939.[268] The facilities were being expanded aggressively, a process that included building several wooden huts on the grounds of the estate. Secondly, Knox was "notorious for not telling anyone anything."[269] Finally, the work in Bletchley Park was highly compartmentalized and for good reason. Very few individuals were capable of or entrusted with the responsibility of knowing about the entirety of the operation at Bletchley Park. The compartmentalization allowed for more focused concentration on specific tasks and no overlapping, which is what Welchman did on accident. He would later refer to this first thought he had as a "lead balloon."[270]

This lead balloon is important because it helped fuel Welchman's further ideas. This first failed brainstorm was important because it gave birth to two more successful ideas. Welchman's next idea largely concerned the staffing of Bletchley Park, or lack thereof. By assuming that the British were going to break the code, Welchman knew that Bletchley Park eventually would

[267] Welchman, *The Hut Six Story*, 73.
[268] *Ibid.*
[269] *Ibid.*, 72.
[270] *Ibid.*

need more intercept operators, intercept coordinators, and decoding personnel.[271] Welchman took his ideas to Commander Edward Travis, deputy director of Bletchley Park. Welchman told Travis that Bletchley Park needed to expand in order to handle any and all volume of Enigma traffic twenty-four hours a day. In order for the staff to efficiently handle this volume of traffic they would have to be proficiently organized. Welchman proposed that there be five departments, a chain of different organizations that would systematically solve code.

The Registration Room studied traffic analysis around the clock, and was fed information from radio intercept stations across Britain. The Intercept Control rooms would maintain constant contact with the radio intercept stations and focus on the most valuable traffic.[272] Next there was a Machine Room that handled the decoding of the messages relayed to them from the Registration and Interception rooms. If the staff of the Machine Room thought that there was a particular crib that warranted trying they would pass their information to the Sheet-Stacking Room, where they would look for patterns in the transmissions.[273] If this crib was successful, the code was passed onto the Decoding Room, which would finish the process. Commander Travis was overwhelmingly supportive of Welchman's idea to streamline the process at Bletchley Park and the result was the expansion of facilities and staff.

The expansion of the facilities at Bletchley Park represented one of the greatest fundamental differences between British and Polish codebreaking operations. The British enjoyed the benefit of a high-pressure war time atmosphere which enabled them to tap into the financial resources required to build up the facilities at Bletchley Park. Progress came much faster when accompanied by a blank check. The lack of resources was one reason the Poles had

[271] *Ibid.*, 75.
[272] *Ibid.* 76-77.
[273] *Ibid.*

not been able develop the *bomba* effectively or produce Zygalski sheets in enough numbers to be effective. Three things effectively killed the Polish *bomba*, the change in German transmission protocol in May 1937 and the addition of more wheels in September 1938 and, more importantly, the lack of funding to develop it. The Poles had accomplished much with what they had, but did not have the finances or personnel for further progress. The British were able to finance their codebreaking project considerably better than the Poles. There were two significant reasons for this: firstly, the government of Britain had the means, and secondly, they had come to understand the importance of codebreaking during the First World War. Poland, as a new nation, lacked both of these pivotal traits. In addition to Bletchley Park being better funded, it was physically larger. Even before Welchman's idea to expand the facilities at Bletchley Park, the British codebreaking operation was larger than the Polish program ever was. From the onset of the Second World War the British had a significant advantage over the Poles despite being exposed to the code for considerably less time.

Alan Turing may have been the brain-child of the initial British bombe, but Gordon Welchman offered a tremendous addition to the machine.[274] This was the second of Welchman's ideas following the "lead balloon" and it was also the most important. Welchman's addition came in the form of the "diagonal board."The diagonal board was a 26 x 26 grid of terminals.[275] Each of the four sides of the board was labeled with the twenty-six letters of the alphabet. The test register and scramblers of the bombe were connected to the diagonal board. There were sockets on the diagonal board. If the codebreakers wished to test all of the possibilities for the letter 'E' they would run plug-in wires from all twenty-six 'E's that made up the row to the

[274] Cooper and J. van Leeuwen. *Alan Turing: His Work and Impact*, 431.
[275] Welchman, *The Hut Six Story*, 301.

twenty-five plug-ins for the other letters in the alphabet.[276] This addition to the Bombe meant that the machine could further reduce the number of plausible starting keys in fewer numbers of runs using different variations found in the crib method.[277]

The diagonal board would increase the processing power of the bombe significantly. Welchman initially designed the diagonal board by drawing a simple wiring diagram and taking it over to Turing.[278] Turing was initially incredulous when he first looked over the diagram, but agreed with Welchman that it could, in fact, be done and that it would boost the processing ability of the bombe substantially. With Turing's approval, Welchman was able to take his idea for the diagonal board to Commander Travis.[279] Welchman began to closely coordinate with Harold Keen at BTM in order to equip the new bombes with the diagonal board. The results were substantial. Welchman wrote that "the vast number of stecker combinations (around 200 trillion) on which the German cryptographers probably pinned their faith was of no avail against the bombe."[280]

The bombe was now equipped with a four-step capabilities. In order for the bombe to remain practical it would have to possess incredible processing power. It would need to be capable of cycling through twenty rotor positions per second and averaging a half-million rotations in a few hours.[281] A finished bombe was equipped with thirty rotating drums that symbolized the rotors of ten Enigmas.[282] When the Bombe reached a possible key the machine would come to a stop. Each stop was recorded and then the letters were run through a single

---

[276]*Ibid.*, 303-04.
[277] *Ibid.*,.
[278] *Ibid.*, 81.
[279]*Ibid*.
[280]*Ibid.*, 82.
[281] Hodges, *Alan Turing: The Enigma*, 184-5.
[282] Smith, "How it Began: Bletchley Park Goes to War," 32.

replica Enigma to see if they were correct. If they were correct, it would result in turning the plaintext message into German.[283]

The bombe drastically reduced the numerical advantages the Germans took such pride in. The efficiency was bolstered further by the process of sheet stacking. When duplicate patterns were detected by the bombes, they were charted on large sheets—similar to, but larger to the Zygalski sheets—and the sheets were stacked atop one atop another so that analysts could find more concrete patterns in the transmissions. Welchman wrote that British success stemmed, in part, from the blind spots of the Germans. "Professional codebreakers," wrote Welchman "no matter how good they are, may fail to see how a mind with a different background might find a way of defeating them."[284] Welchman seems to have placed a tremendous emphasis on the different perspectives that the British were able to bring to the process. This quote reflected the diversity of the minds working on the Enigma problem; breaking the code was only possible through the diversification and compartmentalization of these various and talented persons. The development of the bombe changed the tide of the war in many ways for Britain.

The Turing-Welchman bombe was the foundation for the rest of Bletchley Park operations from 1940 onwards. The development could not have come at a better time. By May 1940 the S*itzkrieg* (Phony War) had ended and the Germans had unleashed their full military might on western Europe. In a matter of months the Germans had steamrolled through Denmark, the Low Countries, and France.[285] Britain now stood alone, with Nazi Germany across the narrow English Channel. By August the Luftwaffe was bombing Britain day and night. At first the Luftwaffe sought to destroy the Royal Air Force on the ground by attacking airbases across

[283] *Ibid.*.
[284] Welchman, *The Hut Six Story*, 82.
[285] McKay, *The Secret Lives of Codebreakers*, 107-108.

southern England. Herman Goering quickly changed his mind after a few weeks of stiff RAF resistance and then shifted the focus of his strategy to bombing British cities. The goal was to bomb the British civilians into submission. The British were aided in a number of ways in their battle against the Luftwaffe. In addition to radar the British were able to utilize the Turing-Welchman bombe to crack the Luftwaffe code and intercept sorties of German bombers before they reached their targets.[286]

The German bomber crews received transmissions en route to their targets in Britain, which were intercepted by forward radio stations and passed onto the codebreakers at Bletchley Park. The radio transmissions were vital in keeping German aircraft on course. The codebreakers did not succeed in decrypting every aspect of the message, such as specific targets names, but they were able to identify a small number of potential targets and the number of aircraft that were involved.[287] Based on this information the Air Ministry "bent" radio waves, a technique which would cause German bombers to veer off course and drop their bombs on the wrong targets.[288] It was not an exact science, but when the bending of radio waves was combined with the tenacity of the Royal Air Force fighters, the German aerial offensive was blunted significantly. Even though codebreakers were able to aide in the fight against the Luftwaffe in the Battle of Britain they still strove to be more accurate. The early years of wartime British codebreaking were filled with the desire for exactness, this would spur the codebreakers forward throughout the early years of the war.

The bombe and the codebreakers at Bletchley Park also played a vital role in monitoring the development of Operation Sea Lion, the proposed invasion of Britain. It was through the

[286] F.W. Winterbotham, *The Ultra Secret* (New York, NY: Harper and Row, 1974), 40-45.
[287] Sinclair, *The Secret Lives of the Codebreakers,* 110-111.
[288] *Ibid.*

monitoring of German radio traffic that Britain was able to prepare for invasion on such short notice. On one occasion, 7 September 1940, the British Home Guard went into full alert after the issue of Invasion Alert No. 1, codenamed Cromwell.[289] It was after scanning the German decrypted messages that the British discovered that Sea Lion had been cancelled. The Battle of Britain and Operation Sea Lion went hand in hand. By stymieing the German efforts to establish air supremacy the British were able to simultaneously thwart the amphibious invasion of Britain. Without the ability to establish an umbrella of air control over the island, the German invasion plans were not able to take serious root.

In the Battle of Britain and Operation Sea Lion, the Turing-Welchman bombe and the staff of Bletchley Park had help saved Britain twice. They would eventually succeed in saving the nation a third time. Turing and the staff of Bletchley Park also broke the incredibly complex naval code, which was utilized by the German submarine fleet. Since the outbreak of the war German U-boats had been plaguing the British convoys crisscrossing the Atlantic. The German navy was attempting to strangle Britain's supply lines and starve the country to death. The German navy had attempted to accomplish a similar task during the First World War, but had failed to succeed. By the Second World War the German submarine force was more effective and much larger. At the war's beginning, Germany had fifty-seven submarines available for service.[290] The threat to allied shipping in the Second World War was substantially higher than in the First. The pressure in Britain was mounting steadily. By 1942 convoy losses were staggering and the British were in desperate need of a way to predict the movements of German U-boats.

---

[289] Winterbotham, *The Ultra Secret*, 56.
[290] Kozaczuk, 196.

Throughout 1941 the British lost 131,583 tons of shipping per month on average to submarines in the Atlantic Ocean.[291] Prior to this, the British codebreakers had broken the Luftwaffe, army, and diplomatic codes, but had not been able to make much progress against the German naval ciphers. As mentioned before, the German navy had more wheel combinations to choose from and took extra precautions in protecting their transmissions. It was not until mid-1941 that the British began to make headway against the German naval code. By this time the number of German submarines operating had increased drastically in comparison to the number available at the beginning of the war. By October 1942 there were seventy U-boats in operation, and three months later there were 100.[292]

The codebreakers at Bletchley Park were not able to rely on the same results they had encountered when breaking the air force code. The approximate accuracy that had served the British well enough during the Battle of Britain was simply not good enough. The British were aided substantially in their quest to break the naval code in May 1940. On 30 May the German submarine U-13 had navigated its way through British coastal minefields and pastthe HMS *Weston* off the coast of Suffolk.[293] U-13 had managed to pilot through the minefields by capturing charts from the HMS *Seal*, a British submarine that was damaged and eventually captured shortly following the evacuation of Dunkirk.[294] After the *Weston* ascertained that U-13 was an enemy vessel—the German craft had not responded to signals from the *Weston*, which mistook her for being an Allied submarine—the British warship began its pursuit.[295] After several hours of depth-charging U-13 began taking on water and the submarine's captain, Max

[291] MFQ 586/7/372, Graph showing allied Shiiping Losses and Cause of Loss, 1941-42, London, November, 1942.
[292] Kozaczuk, 196-97.
[293] Serbag-Montifore, *Enigma: The Battle for the Code*, 83.
[294] *Ibid.*
[295] *Ibid.*

Schulte, ordered the vessel to surface. At 2 a.m. on 31 May U-13 briefly surfaced and was then scuttled.[296] The British were not able to capture any material from U-13, but its sinking spurred a change in German naval communication policy. Admiral Karl Dönitz, commander of the German U-boat force, feared that the British may have acquired some Enigma manuals from U-13 and ordered that from then on submarine crews would carry manuals printed with water soluble ink.[297] This change would make the likelihood of the British grabbing Enigma codebooks off a submarine almost impossible. Yet, the British desperately needed to lay their hands on a physical copy of the Enigma codebook.

It took the British more than a year following the scuttling of U-13 to obtain the coveted Engima codebooks. By late April 1941 the Admiralty had become increasingly desperate in this quest. They suggested that the Royal Navy hunt German trawlers north of Iceland.[298] German trawlers regularly patrolled this area in order to observe and report on weather patterns in the North Atlantic. One such trawler was targeted, the *München*.[299] At 3 p.m. on 7 May 1941 HMS *Somali* spotted the *München,* and gave chase. This was not the first time the *Somali* had embarked on a mission of this nature.

The crew of the *Somali* had made a similar attack to capture another German weather trawler, the *Krebs,* in March 1941. The boarding party of the *Somali* had boarded the *Krebs* off the coast of Norway and managed to secure two Enigma wheels and the settings for German home waters.[300] The wheels were transported to Bletchley Park where they were studied and proved to be of some use. Still the codebreakers could only use the wheels and the settings to

[296] *Ibid.,* 84-85.
[297] *Ibid.,* 86-87.
[298] *Ibid.,* 128.
[299] *Ibid.*
[300] *Ibid.,* 118.

decode messages from February.[301] The February messages, though, could not be read quickly enough. This happened for two reasons: firstly, the captured components were not delivered to Bletchley Park until 12 March, eight days after their seizure. Secondly, many of the messages sent in February were dummy signals composed almost entirely of consonants.[302] The consonants made it nearly impossible for the codebreakers to find patterns in the recorded traffic. Wading through the clutter of dummy messages wasted valuable time. Many of the messages from February were not translated until the beginning of May. The codebreakers had discovered another piece of the Enigma puzzle, but it had cost them more precious time.

The capture of the *München* changed matters considerably in the race for the naval code. Sailors from the *Somali* successfully boarded her and took the crew prisoner without suffering any casualties. A second boarding party, coming from the supporting destroyer HMS *Edinburgh*, confiscated an Enigma codebook.[303] The codebook was a gold mine. Unlike the codebooks confiscated from the *Krebs*, the *München* possessed codebooks for May and June.[304] Now the British were able to use the captured materials to decrypt current messages. The British codebreakers received another boon from the Royal Navy when U-110 was captured on the surface in 9 May.[305] During a convoy attack the submarine had been viciously depth-charged by the HMS *Aubretia*. After surfacing, U-110 was rammed by the HMS *Broadway* in an effort to keep her from submerging again. Shortly after U-110 was rammed, a boarding party from HMS *Bulldog* descended onto the crippled submarine in search of signal books. The crew had abandoned ship shortly following the collision with *Broadway.* The Germans had failed to set

---

301 *Ibid.,* 120-121.
302 *Ibid.,* 119-20.
303 *Ibid.,*130-131; Calvocoressi, *Top Secret Ultra,* 86.
304 Serbag-Montefiore, *Enigma: The Battle for the Code, 130-131.*
305 *Ibid.,* 132; Calvocoressi, *Top Secret Ultra,* 86.

scuttling charges before abandoning the ship.[306] The boarding party discovered a functioning Enigma, rotors, and an entire set of codebooks. The materials were quickly transported to Bletchley Park, and along with the manuals from the *München*, provided the British with a suprising new wealth of physical intelligence to draw from.

The effects of the captured materials on research were immediate. A report on Naval Enigma interception contains a curt, yet revealing summary of Bletchley Park's efficiency in the month following the seizure of material from *München* and U-110: "All German Naval traffic (Home-waters) read currently from 1st June 1941, as a result of a capture."[307] There was a noticeable change in efficiency in decrypting the naval code. Every daily key was broken in April, twenty-one days were broken in May, while June and July's daily keys were all decrypted as well. In a span of 122 days, Bletchley Park was able to break the daily key 113 times, resulting in a 92.6 percent average.[308] In the latter half of 1941 the codebreakers effectiveness decreased one percent, but their progress was exceptional. From August to December they only failed to break the daily key thirteen times, a 91.6 percent average.[309] In addition to this, the time-lag between decryptions lowered incredibly from fifty hours in August to 27 hours in November. It should also be noted that during the same time period the number of bombes on-site at Bletchley Park increased from seven to sixteen.[310] The statistical correlation between the number of bombes and the decrease in lag-time cannot be ignored: the number of bombes operating nearly doubled and the lag-time decreased by almost fifty percent.[311]

[306] Serbag-Montefiore, *Enigma: The Battle for the Code*, 140-141.
[307] HW 50/70, Naval Enigma-Travel Statistics and Notes on breaks, London, 1945.
[308] *Ibid.*
[309] *Ibid.*
[310] *Ibid.*
[311] *Ibid.*

The number of bombes on-site at Bletchley Park continued to grow substantially, and the number of messages decrypted rose in correlation. This was the realization of a goal established by Frank Birch early in the war. On 21 December 1940, Birch wrote "The chances of reading current Enigma depends ultimately on the number of bombes available. The pundits promise that given 35 bombes they guarantee to break Enigma continuously at an average delay of 48 hours."[312] By December 1942 there were forty-nine bombes operating, a year later seventy-three.[313] During these years the number of naval messages decrypted also grew substantially. In 1942 148, 196 messages were decrypted in ten months, an average of 14,819 per month.[314] The following year 370,861 naval messages were decrypted over twelve months, allowing for a monthly average of 30,905 messages decrypted.[315] By 1942 the British were reading the German naval code with regularity, although they continued to suffer temporary setbacks that extended into early 1943. The U-boat flotilla began to lose its control in the Atlantic steadily during the latter half of 1942.

The noticeable change in Bletchley Park's efficiency becomes even more remarkable when one considers that U-boats added a fourth wheel in 1942.[316] The addition of a fourth possible wheel increased the variables of decryption greatly. This addition did not, however, foil the men and women at Bletchley Park. As early as 1941 the British had intelligence that indicated that the German U-boat flotilla would be transitioning to a four wheel system. "The introduction of the 4th wheel did not catch us by surprise," Mahon wrote. With the aid of up-to-date intelligence the cryptologists at Bletchley Park were able to adjust their calculations when analyzing U-boat signals. By 1942 the British were able to work through the basic German

[312] *Ibid.*
[313] *Ibid.*
[314] *Ibid.*
[315] *Ibid.*
[316] *Ibid.*

signals and even handle variables with relative ease. It had taken more than three years, but the British had been able to rise to occasion and break the code.

The Polish codebreakers had outlined a fundamental idea for the British to build off of: an electro-mechanical device that would assist codebreakers in sorting through the massive amount of coded transmitted messages. Government Code & Cypher School became an incubator for the brilliant minds of Turing, Welchman, Knox, Keen, Twinn, Denniston, and countless others. They arrived at the same strategy as the Poles. Under Turing's initial strong leadership, the British were able to focus their efforts on creating a bombe that would carry the cryptological burden. Welchman's diagonal board greatly improved Turing's original design and after several months the process was refined with the aid of codebooks and Enigma parts captured from various German vessels. The seizure of the up-to-date intelligence combined with the massive financial resources made available to GC & CS allowed for the codebreakers to progress their methods rapidly. In a little over four years the British codebreakers had gone from in the dark to reading German radio traffic with relative ease and accuracy. By following a formula perfected during the First World War, recruiting the finest minds and obtaining up-to-date intelligence, the British had engineered a mechanical device that predated modern computers. Once again, Britain had been saved by a group that started as bumbling amateurs, but had evolved into the keenest codebreakers in the world.

CHAPTER 5

CONCLUSION

"Everyone has won, and all must have prizes."

—Lewis Carroll, *Alice's Adventures in Wonderland*

The staff at Bletchley Park remained busy for the remainder of the war. The breaking of the Enigma code was not an end-all solution. Every day for the remainder of the conflict the men and women of Bletchley Park toiled to decrypt German transmissions and send the intelligence garnered from the messages to the airmen, soldiers, and sailors in the field. There is no way to accurately calculate the lives that the staff of Bletchley Park saved by breaking the code. Perhaps that is why many of the key personnel were awarded knighthoods for their actions. Even though these honors were given under the cloak of state secrecy and their deeds were classified, the codebreakers themselves knew how much was won and lost in the confines of that country estate in Milton Keynes. Theirs was a vital part of contributing to the overall Allied victory which came, at long last, on 8 May 1945. Supreme Allied Commander Dwight D. Eisenhower estimated that the men and women of Bletchley Park shortened the war by two years.[317]

Sinclair McKay wrote even following the 1974 publication of Winterbotham's account that "Bletchley-ites could not bring themselves to even mention the place, let alone discuss their roles there."[318] In the years and decades following the Allied victory many of the former codebreakers lied to family and professional acquaintances about war time work. Despite the temptation to tell parents or loved ones, they ceded to the oath they swore. Some of them, even

[317] McKay, *The Secret Lives of Codebreakers*, 322.
[318] *Ibid.*

when confronted directly about working at Bletchley Park, refused to speak. The Official Secrets Act of 1911 bound many of the codebreakers to their graves.

Alan Turing never told anyone about his role at Bletchley Park. Even after being made the youngest Fellow Royal Society and being awarded an O.B.E Turing remained silent. In 1952 Turing was arrested and convicted for gross indecency for having homosexual relations, then a criminal offense in Great Britain.[319] Instead of serving a prison sentence, Turing elected to be chemically castrated. There has been endless speculation as to whether or not the castration led to Turing's suicide, but there is no way of knowing for sure. One must wonder whether or not Turing's wartime work, had it been revealed during the time of his arrest and trial, could have saved him from the castration, and possibly his suicide. He had signed the Official Secrets Act of 1911, however, and he kept his oath. It was not until December 2013 that Turing received a posthumous royal pardon for his crime.[320] The pardon, in combination with the release of the film *The Imitation Game* in which Turing is portrayed by Benedict Cumberbatch, has led to the increased popularity of Turing and his work at Bletchley Park.

What happened at Bletchley Park during the Second World War was not entirely innovation. In some part, the British followed a proven formula. The senior officials at GC&CS followed the recruiting patterns they had relied on during the First World War. With these minds in place, and with the help of up-to-date intelligence procured from multiple sources, Turing, Welchman and countless others were able to develop the bombe. The bombe eliminated enough of the variables and allowed the British to break the codes using pattern recognition.

---

[319] *Ibid.*, 299.

[320] "Royal Pardon for codebreaker Alan Turing," BBC NEWS, published 24 December 2013, http://www.bbc.com/news/technology-25495315 (accessed 15 January 2015).

The invasion paranoia that gripped Edwardian Britain had led to the creation of British Intelligence. The outbreak of the First World War saw the establishment of Room 40. It was during 1914-18 that the British learned the two most critical aspects of codebreaking: the recruitment of intelligent personnel and the acquisition of current intelligence. Following the war, the Germans adopted a highly-complicated communication system. The Poles got an early jump on breaking the Enigma code, and through almost pure mathematical reasoning, broke an early version of the code. Their progress went unreported until August 1939 and thusly, made no significant contribution to the overall British strategy. By recruiting like-minded personnel as the Poles, the British were able to create the technology necessary for breaking the Enigma code.

By synthesizing trusted practices from the First World War and new technologies born of necessity, a group of British amateurs were flung together into the intensity of a war time pressure cooker, and managed to find the solution to what was perceived as an unbreakable code. The process of breaking that code was filled with endless experiments conducted by the British and the Poles. In the end, the British proved capable of finding the solution to the Enigma quandary.

BIBLIOGRAPHY

Primary Sources

National Archives (Kew), ADM 1/23899: Copy of speech given by Alfred Ewing entitled "Some Special War Work: A Lecture to the Edinburgh Philosophical Institution," Edinburgh, 13 December 1927.

"Bethell letter." https://www.sis.gov.uk/our-history/bethell-letter.html. Accessed 18 March 2014.

Calvocoressi, Peter. *Top Secret Ultra*. New York, NY: Pantheon Books, 1980.

Carpenter, B.E. and R.W. Doran, editors. *A.M. Turing's ACE Report of 1946 and Other Papers.* Cambridge, MA: The MIT Press, 1986.

"General Russell on Possible Invasion," *The Aberdeen Daily Journal,* 2 January 1909. Accessed from the Newspaper Collection at the British Library.

"German spies in Scotland: Whole Country's Defences are Known to Berlin, System of Espionage Exposed." *Dundee Courier,* 27 January 1909. Accessed from the Newspaper Collection at the British Library.

Hinsley, F.H. *British Intelligence in the Second World War: It's Influence on Strategy and Operations*. New York: Cambridge University Press, 1979.

MEPO 3/1106, Materials related to the Landsbury Case, London, March 1934.

NA HO 317/43 Letter to Colonel Warde, London, 612 May 1906.

NA HW 3/3. Manuscript entitled *History of Room 40 O.B.* written by William F. Clarke, manuscript, London, 2 July 1951.

NA HW 3/77, "Zimmerman Telegram: A footnote to Friedman's Account" by Nigel de Grey, London, 31 October 1945.

NA HW 3/179, Memorandum regarding the Zimmerman Telegram, London, 24 February 1917.

NA HW 3/182, Letter by O.A.R Murray, London, 16 December 1927.

NA HW 25/6, Communication from Alistair Denniston to the Secretary of the Air Ministry, London, 1 July 1924.

NA HW 25/6, Communication from *Enigma Chiffriermaschinen Aktiengesellschaft* about price and models available for order, Berlin, 2 June 1924.

NA HW 25/6, Communication from Henry Tom to E.T.F Crowe, London, 31 January, 1925.

NA HW 25/6, Communication from J.H. Herring to Secretary of Air Ministry about Enigma Instruction Booklets, Berlin, 19 June 1924.

NA HW 25/6, Report on Enigma machine from Government Code & Cypher School, London, 16 March 1926.

NA HW 25/8, Enigma Instruction Booklet written in German, English translation attached, London, 1923.

NA HW 25/12, Letter from Knox to Denniston about Tri-Lateral Meetings in Warsaw, London, July 1939

NA 25/12, Report by D. Knox on Tri-Lateral Meeting in Warsaw, London, 4 August 1939.

NA HW 25/16, Report written by S.A. Mayer entitled "The breaking up of the German Ciphering machine "ENIGMA" by the cryptological section in the 2nd Department of the General Staff of the Polish Armed Forces" London, 21 June 1977.

NA HW 72/1, Letter from A.G. Denniston to Quarmby at the Foreign Office, London, 22 April 1939.

Reginal Glossop, “Invasion of Britian: Imaginary Conversations and Instructions of the German General Staff,” *The Daily Mail*, 14 November 1906. Accessed from the Newspaper Archive at the British Library.

“The Room 40 Compromise.” http://www.nsa.gov/about/cryptologic_heritage/60th/interactive_timeline/Content/1960s/documents/19600101_1960_Doc_3978516_Room40.pdf. accessed 19 March 2014.

“Treatise on the Enigma, by A.M. Turing”, Alan Turing Catalogue http://www.alanturing.net/turing_archive/archive/b/B05/B05-001.html (accessed 19 December 2014).

The Turing Digital Archive, “A.M. Turing, h.1926-31)” published in *The Shirburnian*, Summer Term 1954, http://www.turingarchive.org/viewer/?id=452&title=6 (accessed 19 January 2015).

The Turing Digital Archive, “Dr. Alan Turing: An Appreciation,” published in the *Manchester Guardian*, 11 June 1954, http://www.turingarchive.org/viewer/?id=452&title=10b (accessed 19 January 2015)

“Official Secrets Act 1911.” http://www.legislation.gov.uk/ukpga/Geo5/1-2/28/contents. Accessed 21 March 2014.

The Turing Digital Archive, *About Alan Turing*, *http://www.turingarchive.org/about/*, accessed 18 January 2014.

Welchman, Gordon. *The Hut Six Story: Breaking the Enigma Codes*. New York, NY: McGraw Hill, 1982.

Winterbotham, F.W. *The Ultra Secret*. New York, NY: Harper and Row, 1974.

Secondary Sources

“Alan Turing.” *Encyclopedia Britannica*. http://www.britannica.com/EBchecked/topic/609739/Alan-Turing, (accessed 21 August 2014).

“Allied Merchant Ship Losses, 1939-43,” American Merchant Marine at War, http://www.usmm.org/wsa/shiploss.html, (accessed 11 December 2014).

Andrew, Christopher. *The Defence of the Realm: The Authorized History of MI-5*. New York: Allen Lane, 2009.

________________. *Her Majesty's Secret Service: The Making of the British Intelligence Community*. New York: Penguin, 1985.

Andrew, Christopher and David Dilks, ed. *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*. Urbana & Chicago: University of Illinois Press, 1984.

Batey, Mavis. *Dilly: The Man Who Broke Enigmas.* London: Biteback, 2009.

Beesly, Patrick. *Room 40: British Naval Intelligence 1914-18*. New York: Harcourt Brace Jovanovich, Publishers, 1982.

Cooper, Barry S. and J. van Leeuwen. *Alan Turing: His Work and Impact.* Walden, MA: Elsevier Science, 2013.

Copeland, B. Jack, ed. *Alan Turing's Automatic Computing Engine: The Master Codebreaker's Struggle to Build the Modern Computer.* New York, NY: Oxford University Press, 2005.

_____________. *Colossus: The Secrets of Bletchley Park's Code-breaking Computers.* New York, NY: Oxford University Press, 2010.

Denniston, Robin. *Thirty Secret Years: A.G. Denniston's work in signals intelligence, 1914-44*. Great Britain: Polperro Heritage Press, 2007.

Erskine, Ralph and Michael Smith, eds. *The Bletchley Park Codebreakers: How ULTRA Shortened the War and Led to the Birth of the Computer.* London: Biteback, 2011.

Ferguson, Niall. *The Pity of War: Explaining World War I.* Great Britain: Basic Books, 1999.

Fitzgerald, Penelope. *The Knox Brothers*. London: Flamingo, 1977.

Frederick Sleigh Roberts, Oxford Dictionary of National Biography, http://www.oxforddnb.com/view/article/35768?docPos=1 (accessed 17 August 2014).

Gannon, Paul. *Colossus: Bletchley Park's Greatest Secret.* London, UK: Atlantic Books, 2006.

____________. *Inside Room 40: The Codebreakers of World War 1*. Surrey, United Kingdom: Ian Allan Publishing, 2010.

Hawking, Stephen, ed. *God Created the Integers: The Mathematical Breakthroughs That Changed History.* Philadelphia, PA: Running Press, 2005.

Hill, Marion. *Bletchley Park People*. Gloucestershire, UK: Sutton Publishing, 2004.

Hodges, Andrew. *Alan Turing: The Enigma*. New York, NY: Simon and Schuster, 1983.

_______________. *Turing: A Natural Philosopher.* London: Phoenix, 1997.

Hoy, Hugh C. *40 O.B. or How the War Was Won.* London: Hutchinson & Co., 1932

Jeffery, Keith. *The Secret History of MI6.* New York: Penguin, 2010.

Jeffrey-Jones, Rhodri. *In Spies We Trust: The Story of Western Intelligence.* Oxford: Oxford University Press, 2013.

Kahn, David. "Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects." *The Historical Journal.* 23, No. 3 (Sept., 1980). Pp. 617-639.

___________. "The International Conference on Ultra." *Military Affairs*. 43. No.2 (Apr., 1979). Pp. 97-98.

___________. "World War II History: The Biggest Hole." *Military Affairs*. 39. No.2 (Apr., 1975). Pp. 74-76.

Keegan, John. *Intelligence in Warfare: Knowledge of the Enemy from Napoleon to Al-Qaeda*. London: Pimlico, 2004.

Kozaczuk, Wladyslaw. *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two.* Ed. And Trans. By Christopher Kasparek. Ann Arbor, MI: University Publications of America, Inc., 1984.

LeQueux, William. *The Bomb Makers: Being some Curious Records concerning the Craft and Cunning of Theodore Drost, an enemy alien in London, together with certain Revelations regarding his daughter Ella.* *http://www.gutenberg.org/files/41132/41132-h/41132-h.htm*. (accessed 4 August 2014).

Lewin, Ronald. *Ultra Goes to War: The First Account of World War II's Greatest Secret Based on Official Documents.* New York: McGraw-Hill Book Company, 1978.

McKay, Sinclair. *The Secret Lives of Codebreakers: The Men and Women Who Cracked the Enigma Code at Bletchley Park.* London, UK: Penguin, 2010.

Richmond, John. "Classics and Intelligence." *Classics Ireland*. Volume 9 (2002).

Rohwer, Jurgen. "Signal Intelligence and World War II: The Unfolding Story." *Journal of Military History*. 63. No. 4 (Oct., 1999). Pp. 939-951.

"Royal Pardon for codebreaker Alan Turing," BBC NEWS. Published 24 December 2013. http://www.bbc.com/news/technology-25495315 (accessed 15 January 2015).

Sebag-Montefiore, Hugh. *Enigma: The Battle for the Code*. Chichester, UK: John Wiley & Sons, Inc., 2000.

Smith, Michael. *Station X: The Codebreakers of Bletchley Park*. London, UK: Pan Books, 1998.

Tuchman, Barbara. *The Zimmerman Telegram*. New York: The Macmillan Company, 1958.

Turing, Sara. *Alan M. Turing*. Cambridge, UK: W. Heffer & Sons, Ltd., 1959.

VITA

ANDREW J. AVERY

Education:	B.A. History, Flagler College, St. Augustine, Florida, 2013 M.A. History, East Tennessee State University, Johnson City, Tennessee, 2015
Professional Experience:	Assistant to Dr. Leila al'Imad, Fall 2013 Assistant to Dr. Andrew Slap, Spring Semester, 2014, HIS 2020 U.S. History since 1877 Assistant to Dr. Andrew Slap, Fall Semester, 2014. Instructor, Spring Semester, 2015.
Honors and Awards:	Tuition Scholarship, East Tennessee State University, 2013-2015 Dean's List Phi Alpha Theta

.