INTRODUCTION

THE TRAITOR IN OUR MIDST

Enigma's Decipherment and Ultra Intelligence

> . . . it is contended that very few Armies ever went to battle better informed of their enemy . . .
>
> – Brig. E. T. Williams' report on British use of signals intelligence, October 1945

In 1974, after decades of secrecy, the British government finally admitted its World War II intelligence service had read thousands of German messages encrypted by the Enigma machine cipher.[1] The intelligence derived from these decrypted messages traveled under the code name "Ultra" (for Ultra Secret) and influenced nearly all of the major battles in the Western theater. Now readers can find histories of Ultra's role in battles across the Atlantic, North Africa, the skies over Britain, and occupied Europe.[2]

Less public attention has been spent on how the Allies obtained these signals decrypts. Many early accounts of the breaking of Enigma have proved to be incomplete or erroneous and have been superseded as more information appeared in the 1980s and 1990s. Now, through various sources, the public can learn the history of Enigma's development and downfall.

Enigma emerged after the end of the First World War as one of several similar electro-mechanical enciphering ideas emerging in the U.S. and Europe. The Dutch inventor, Hugo Alexander Koch, apparently saw his secret-writing machine idea as a tool for a business world needing a relatively uncomplicated yet effective method for protecting commercial secrets. He sold the rights to his enciphering machine patent to

German manufacturer, Arthur Scherbius.[3] Scherbius' firm produced the Enigma in the 1920s and trumpeted the machine as portable and easy to use yet statistically highly secure: over 15 million, million (15×10^{12}) possible substitutions for each letter typed into the machine. In 1926, the German Marine (navy)[4] adopted the Enigma cipher machine, with modifications, as its primary cipher system.[5] Soon the Heer (army) followed suit.[6] Over the next several years, German cryptologists improved the cipher machines to tighten their security against decipherment. By the beginning of World War II, each of the branches of the German military, the police, the railway, civilians, and the Nazi Party were using their own variations of Enigma.

Although the Germans continued to believe their signals impregnable, the Allies captured and stole cipher key settings, found and exploited Enigma's weaknesses, built a rudimentary computer, and broke into virtually every German cipher net. For the first time in history, not just individual codes but an entire system of encipherment was broken.[7]

This successful assault on Enigma's secrets began in the 1930s. Polish intelligence[8] attacked the machine analytically, reconstructing Enigma's internal and rotor wirings from the signals they received. With these reconstructed wirings and a few key documents turned over by a spy, Polish cryptanalysts built their own Enigma facsimiles. They linked several of the reconstructed rotors together to create "Bombes," electromechanical aids capable of checking possible solutions far more quickly than humans. When Adolf Hitler's attack threatened, the Poles passed their decrypting techniques and Enigma models on to the British and the French. The poles soon fled the advancing German army, only to continue working from France until the Germans occupied Vichy France in November 1942. By 1939, the British had organized a section of the Government Code and Cypher School (GC&CS) at Bletchley Park (or BP) to work exclusively on radio intercepts. There, in 1940, the first British Bombes came into service.[9]

In addition to developing new electromechanical and electronic aids, the Allies exploited the Enigma machine's mechanical and linguistic weaknesses, finding shortcuts to its solution.[10] As the analysts began reading one cryptosystem, they often found clues to other key settings, for example, by tracking weather reports on different networks. The lack of coordination between different arms of the Wehrmacht required

that whole messages sometimes be repeated verbatim in several different cipher keys. When the Allies had a "crib"[11] or a possible text for a message repeated to several commands, they could give it as a "menu" (or potential solution) to the Bombes. With such practices, Bletchley's analysts frequently could decrease their deciphering time.

The most frequently and consistently cracked keys were those of the Luftwaffe.[12] From its first cracking in early 1940, the general Luftwaffe key, "Red," provided almost constant reading material for BP through the war's end. During the Battle of Britain, Polish and Bletchley Park cryptanalysts began reading the main German Air Force (Luftwaffe) key regularly in time to assist Fighter Command.[13] The Allies read the Luftwaffe keys in North Africa from the first day of their introduction, 1 January 1942. The continuity offered by reading the Luftwaffe keys virtually every day for years helped keep Bletchley Park ahead of changes in this and other Enigma nets.[14]

The German Army (Heer and Wehrmacht) keys were cracked after the Luftwaffe's but before the more difficult Naval Enigma (Enigma M), which the Bletchley Park team first broke in August 1941.[15] The Enigma M keys proved the most sophisticated and far more secure than the Luftwaffe and Army keys because of several changes and improvements to the Marine machine. Nonetheless, Bletchley Park read the Home Waters key from 1 August 1941 through the end of the war. The most crucial alteration to Enigma M came in February 1942 when the Marine instituted a four-rotor Enigma for the U-boat cipher Triton (Shark to the Allies). Only nine months later, in December 1942, did Bletchley begin reading Shark again, first with occasional delays, but by late March 1943 with little interruption.[16]

As the number of Enigma networks proliferated, Bletchley's cryptanalysts only increased their successes. A report of work in mid-November 1944 reported breaking 77 percent of Luftwaffe traffic, 18 percent of Army traffic (during a difficult call signs upgrade), 35 percent of SS traffic, and 24 percent of railway ciphers. In March 1944, Bletchley reported work on more than one hundred thousand messages, not including Naval Enigma. Bletchley Park's cryptanalysts solved keys for more than 50 percent of this selection, including 62 percent of Luftwaffe traffic and 30 percent of Heer traffic.[17] At times, the intercepts were solved almost immediately. Often, however, a lack of cribs, tightening of operator

security, or Enigma machine modification would increase Bletchley Park's deciphering delay from hours to days or months.

By 1945, Bletchley Park had identified and attacked most versions of Enigma, defeating more than 200 separate networks of keys, albeit many irregularly or temporarily. The Ultra Secret intelligence from these decrypted signals passed to the Allied military commands under tight security, often attributed to a (notional) secret agent working in German command offices and code-named "Boniface." Commanders could use Ultra information only if they had a second source as a cover story, for example, a POW's interrogation, or a fix on a signal through direction finding (D/F). This secret intelligence at times allowed the Allies to avoid waiting U-boats, anticipate surprise attacks, and send their own troops to the Germans' most vulnerable points.

In a massive Index, each shift at Bletchley Park cross-referenced the information acquired from each decrypted Enigma signal. One could track a particular U-boat or a particular general, and through the succeeding actions speculate on upcoming offensives or the whereabouts of other, not-yet-located divisions or ships. For example, the ship *Schorndorf* was sunk with Ultra's help, not through her own enciphered signals, which were infrequent and not solved, but rather through the deciphered signals ordering two U-boats to support her. With the Index's extensive anthology, the Allies could track components that might not be momentarily important, yet could lead to bigger fish.

A Fatal Blindness

Yet as the Allies pieced together thousands of supply requests, status reports, and direct orders emerging in Enigma decrypts, the Germans seemed not to notice the enemy's intelligence collection. German cryptologic experts touted the high security and reliability of the Enigma ciphers and attributed information leaks to every other possible source, even their own radio operators. Through numerous investigations during the war, intelligence bureaus confirmed Enigma's security and announced the enemy could not regularly read the machine's ciphers.

Even after the war, confidence in Enigma persisted. A Polish book published in 1967 claimed that young cryptologists working for Polish

intelligence before and during World War II had solved Enigma. As word of the book crossed Germany, ex-Wehrmacht officers dismissed its claim of cryptological triumph as "wishful thinking." Not even the historical community considered following up on the tale.[18]

In 1970, the former head of the German Marine's B-Dienst (Beobachtung or Observation Service), Captain Heinz Bonatz, wrote his own history of Germany's intelligence successes.[19] He described the German military and government embracing the latest communications technology, combining Enigma and radios with striking results. In the rapid conquest of country after country, they had relied heavily on nearly constant signals to coordinate the rapid attacks, "which overwhelmed France and might have overwhelmed Britain."[20] Knowing their radio messages would be overheard by enemy ears even long before the war, they had adopted Enigma as the most modern enciphering system of the time.

Bonatz directly answered the claim of Enigma's compromise. He acknowledged that the Allies had seized cipher machines from captured U-boats but insisted nonetheless that the Allies did not and could not have read German ciphers regularly. He explained that "all necessary measures were taken to guarantee the cipher's security, in case a machine should fall into the hands of the enemy."[21]

As further proof, the former B-Dienst chief declares that the Allies "would not have let [Enigma's compromise] go unmentioned." After the war, he had had "numerous conversations with the former enemy's specialists," which had confirmed "that the [Marine Enigma] was secure against break-in and the German naval radio signals could not be read." He was certain the Allies would never have remained silent about such a triumph. "Besides," he continues, "this [ability to read Enigma-encrypted signals] would have been visible in their own sigint [signals intelligence]," which Bonatz's agency had deciphered.[22] Thus, in 1970, after published Polish claims and U.S. admissions of successes solving machine ciphers, Bonatz still entertained no doubts of Enigma's security. The sheer weight of the Allies' continued silence convinced him.

In 1974, the publication of *The Ultra Secret* stating, with approval from a high-level wartime commander, that the Allies had cracked Enigma completely reversed the German position.[23]

A Puzzlement

Why were the revelations of Ultra so astonishing? Why did they catch not only former intelligence officers but the most distinguished historians of cryptology by surprise? How could the Allies use so much secret information from Enigma-encrypted signals and not make the Germans suspect their source?

This book considers the answers to these questions and draws lessons about security, specifically in cryptology and communications. This wartime saga also offers guidelines for setting up an organization for failure or for success in exploiting emerging technologies. Here is the story of the Germans using a sophisticated, technologically advanced communications system and yet losing their grip on both gathering enemy intelligence and securing their own communications. This story also describes the largely British organization whose primarily civilian staff constantly challenged their own and the enemy's security and, in so doing, had unprecedented and so far unequaled success.

German intelligence had its own share of cryptographic and cryptanalytic successes, many of which Captain Bonatz and others touted after the war. Early on, German cryptanalysts had considerable success against the codes of Britain, France, the United States, and the Soviet Union. Given their own success at cracking ciphers, why, as the war progressed, did the Germans never seriously consider their main high-grade cipher system as the source of so many of their problems? An enormous percentage of their enciphered signals depended on a single cipher system. Did they ever consider how completely their communications system could be compromised? How could the Germans have never recognized that Enigma had been broken? How did the Allies manage both to break this "secure" system and to keep the secret of their success so completely for thirty years? Why were the Germans so certain of their machine's security?

Both Enigma's compromise and the extraordinary success of Ultra stem from technical and cultural grounds. Technologically, the world stood on a different plane from our postwar years. Radio was a still new tool for communicating across distances without wires. Computers considered obsolete decades ago seemed a practical impossibility in the 1930s. In the age of punch cards and tabulators, the sheer number of

Enigma's possible letter substitutions with its appearance of randomness implied extraordinary security.

The Allies' remarkable success against this sophisticated electromechanical enciphering machine was first a feat of mathematical and cryptanalytic brilliance. But this triumph goes beyond the actual breaking of the cipher machine. More important than technology, the organization and basic assumptions of the opposing intelligence systems shaped the success of one side and the defeat of the other. In the rapidly changing cryptologic war, intelligence agencies had to adapt quickly to succeed. The Allied agencies managed to do this. German intelligence did not.

This contrast in adaptability stems from the opposing signals intelligence organizations. The structures and cultures in these organizations shaped the ability of intelligence personnel to adapt and respond quickly to the constant changes in the enemy's ciphers. The men and women in intelligence entered the war, began their attacks on enemy ciphers, and considered their own ciphers' compromise, all within the confines of their organization's assumptions about cryptology. Thus, to understand Enigma's defeat, as well as Ultra's success, requires knowing the construction and functioning of the opposing agencies.

We cannot simply dismiss the failure of German intelligence as a direct result of Hitler's National Socialism or some single act of Allied genius or German idiocy. Rather the strengths of the Enigma cipher machine and the flaws of the German signals intelligence organizations combined to create a blind spot that the well-coordinated Allied agencies eagerly exploited.

Finally, Bonatz's words epitomize his peers' attitude toward World War II signals intelligence and Enigma's security during the war and into the present. These intelligence officers maintained a stubborn belief in Enigma's absolute security in the face of considerable evidence to the contrary. The Germans missed numerous clues, overlooked several obvious signs, and succumbed to their own wishful thinking about Enigma. Even their numerous security investigations failed to reveal the weaknesses in the Enigma system, let alone the hemorrhage of information passing to the Allies from Ultra. Their refusal to simply acknowledge mistakes, let alone enlist help to investigate them, would ruin German signals intelligence.

Learning from Defeat

In the end, as we all know, the Germans lost the war. The general public has long attributed both this loss and the war more generally to the evils of National Socialism. So, some may ask, why bother looking at the security investigations of defeated sigint bureaus? Because Nazism played only a minimal role in the signals intelligence war and certainly not a deciding one. The real story is both more mundane and far more important for us today. Ordinary people made the difference. Their belief in possibility and impossibility decided whether they defeated the enemy. They have much to teach the modern user of communications and cryptology.

Although the Allied cracking of Enigma has inspired numerous personal accounts as well as historical analyses of Ultra, modern security enthusiasts will learn more from tracing the causes of Enigma's failure. We can see strong parallels between today and the 1930s and 1940s. Like the commanders in World War II, we must grapple with the advances and perils of more mobile communications. Whether we know it or not, our numerous communications devices – from cell phones to the Internet – all use some form of cryptology. The twenty-first century need for secure communications does not stop with national intelligence staff but extends to companies of every size, their IT experts and financial transactions, right down to the average Internet user.

A similar revolution in communications before and during the Second World War also launched new technologies, new specialties, new business practices, and, of course, new problems. This revolution arose from a convergence of new technologies and industrial methods: wireless radio, electricity, mechanization, mass production, and automation. Cryptography moved from book codes and ciphers to machine ciphers. In turn, cryptanalysis would create new specialties, first in electromechanics and eventually in computer science. Moreover, cryptanalysis in the Second World War would produce rooms full of new machines, enormous production systems, and an appreciation for the ephemeral nature of even machine-based cryptologic security.

Today's technology may be more advanced than shortwave radios and Enigma, but we face the same issues of protecting communications

from unwanted eavesdroppers and recognizing when security has failed. Knowing the dramatic outcome of two different methods of exploiting these new technologies will help us avoid the pitfalls into which German signals intelligence tumbled. This work examines these various snares, including arrogance and complacency about security, as well as the cultural and structural pressures, such as rigid signaling procedures, that limited the success of German organizations and their staffs.

Using recently declassified archival materials, this book compares the organization and practices of the German intelligence agencies with those of the spectacularly successful western Allies. A thorough examination of the various German organizations and their operations explains why no one could acknowledge that their main cipher network had been completely compromised. In contrast, the British increasingly exploited signals intelligence successfully and foiled German signals intelligence by improving cipher security throughout the war.

This work arose from the examination of German, American, and British wartime and postwar documents now housed in the U.S. National Archives, London's Public Record Office, and Germany's Auswärtiges Amt (Bonn) and Bundes-Militärarchiv (Freiburg). As the National Security Agency's (NSA) Scholar-in-Residence, I had access to these recently declassified collections, including the massive Historic Cryptologic Collection (nearly fifteen hundred boxes of documents), U.S. naval intelligence documents, collections of captured documents, POW interrogations, Target Intelligence Committee (TICOM) reports, and wartime and postwar reports. Britain's recent releases include thousands of folders of Bletchley Park memos, reports, histories, and postmortems. These documents allow a partial examination of Allied wartime communications security as a comparison to the German effort.

Through an examination of the German and Allied agencies, this book argues Enigma's defeat arose less from a technological flaw than from the systemic failure of an entire intelligence system. The first three chapters describe the particulars of Enigma and the organizations that handled both Enigma's security and the attacks on enemy systems. Turning to the Allied story, two chapters outline Allied sigint at Bletchley Park and the disguise and dissemination of the Ultra

material. The Germans' concerns about Enigma's security and their investigations into the betrayal of military secrets appear in Chapter 6. Chapter 7 lays out the contrast of Allied communications security practices and responses to potential leaks. Chapters 8 and 9 analyze the underlying reasons for the two vastly different organizations and outcomes, followed by a concluding summary.