WEP Warwick Evans Publishing

Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 12
LHPPR 2024

The Battle of Advantage between Stealing and Decrypting the German Naval Enigma Key in the Battle of the Atlantic (1940-1941)

Hangyu Liang*

The Webb Schools of California, Claremont, United States

* Corresponding Author email: hliang@webb.org

Abstract. In the early years of World War II, German Navy used Enigma to encode messages and prevent their intelligence by Allies. This work considers advantages of stealing and technically decrypting the German Naval Enigma key during the Battle of Atlantic from 1940-41; while Allies had already succeeded in decrypting the German Army Enigma prior to the war. The complexities of Naval Enigma introduced new challenges. Yet British codebreakers persisted with technological decryption — an approach they adopted following their earlier successes. However, details embedded within Naval Enigma plus changes implemented by Germans stood as obstacles against their progress. Solving the encryption required more than what had been previously done. This led them to take an unconventional path: stealing materials related to Enigma. This decision was resource-intensive but it paid off quickly in yielding results that were more practical and morally justifiable than pure decryption efforts made until then. The successful thefts like that which took place during the Lofoten Islands raid and in May 1941 when German ships were captured provided critical Enigma keys and quickened decryption, allowing Allies to obtain valuable intelligence, reroute convoys, and better address the U-boat threat. The work concludes that from a utilitarian perspective stealing Enigma materials was morally justified because it minimized Allied casualties. It also notes that the non-malicious intentions behind theft conformed to deontological principles, underscoring the ethical standing of British actions vis-a-vis Germans'. Ultimately, the British strategy of technological decryption combined with thefts led decisively to turning the tide against Nazis during Battle of Atlantic: hence this paper investigates whether we might perhaps say they were acting ethically (even if illegally) by stealing Enigma-related material.

Keywords: World War II; Enigma cipher machine; Battle of the Atlantic; Cryptanalysis; Intelligence; Utilitarianism; Deontology.

1. Introduction

In 1923, German engineer Dr. Arthur Scherbius invented the Enigma Machine for commercial use [1]. From 1926 to 1930, the German Navy and Army adopted it as the major ciphering system to secure military communication and later applied the Enigma Machine in the Second World War (WWII), aiming to maintain secrecy and gain a tactical advantage over the Allies. The Enigma machine utilized four to five rotating wheels or rotors, each wired in a unique pattern, to scramble plaintext into ciphertext. Additionally, there is a plugboard that allowed letter swapping and a daily changing Enigma key according to codebooks, which combined to create an astronomical number of possible encryption schemes.

Germans held the Enigma Machine with such confidence that they deemed the Enigma Cipher unbreakable because the possible number of keys was higher than even the number of atoms in the observable universe [2]. Germans' strong belief in the communication security created by the Enigma Machines propelled the frequent and constant use of Enigma during WWII. Despite several minor changes during WWII that caused temporary British military information blackouts, the Enigma Machine's working theory remained consistent, including its component mechanism and critical content like daily keys distributed to all German submarines for collaborative communication. The Germans' heavy reliance on Enigma Machines meant that the British codebreakers would have to obtain or acquire their targeted information from the German side either through technological

decryption or theft of the Enigma Machine, as the Enigma Machine only altered slightly from one generation to another.

Unbeknownst to the Germans, after the adoption of the German Army Enigma and before the inauguration of WWII, the Poles, French, and the British successively endeavored to break the Enigma encryption [3]. This early collaborative effort of pure decryption which employed mathematics and technologies laid the groundwork for Allied success in decrypting the German Army Enigma Machine [4]. In 1928, the Poles recognized the Enigma usage in German intercepts through characteristic signs, including infrequently repeated pairs and triplets of letters [5]. Although they did not figure out the exact wiring between the rotors due to time limitations, the Poles solved the German Army Enigma since 1933 and refined their solution afterward. Upon the collapse of Poland in 1939, the Poles distributed their reconstructed Enigma — the Bomba, a device linking six copies of Enigma for an efficient solution — to Britain and France [6]. The interaction with Pole's Bomba and the prior knowledge of Army Enigma layout gave the Allies a great starting point to tackle the German Enigma during WWII [7]. These efforts proved the effectiveness and success in technologically decrypting the German Army Enigma before WWII. As a result, upon WWII's inauguration, British codebreakers employed similar methodologies of technological decryption in subsequent Naval Enigma keys used during the Battle of the Atlantic.

Many historians emphasize the strength of British technological decryption but often overlook instances when this method failed, potentially creating the misunderstanding that the British were consistently strong in decryption and obtained German military secrets smoothly. As is reiterated in various Chinese newspaper and English publications, historians noted the crucial role of the Poles in sharing their early breakthroughs in technological decryption with Britain and France, leading to the development of productive British Bombe Machines, with enhancements later from the United States [3, 8, 9]. Additionally, scholars familiar with the operational theory of the Enigma Machine highlighted the ingenuity of British codebreakers as they exploited the loopholes in German operational errors by inventing the Consecutive Stecker Knock Out to rule out particular Enigma settings [10, 11]. Moreover, comparisons of the British codebreaking effort to Germany's underscore the Allies' superior technological decryption foundation and performance during WWII [5].

During the early stages of the Battle of the Atlantic from 1940 to 1941, British people faced the daunting task of decrypting the German Naval Enigma code. Comparing the merits of these approaches explains why British people preferred employing stealing over pure technological decryption in the Battle of the Atlantic given all the successes they had gained via pure decryption over the previous decade. Pure decryption, while methodical, required substantial resources and often faced setbacks due to the evolving complexity of the Naval Enigma cipher. Conversely, stealing the Enigma key not only required less labor and often offered immediate results, proving more effective and cost-efficient, but also more compelling than pure decryption in terms of morality.

2. The High Stakes of the Battle of the Atlantic

The stakes of the Battle of the Atlantic were incredibly high for Britain, which depended on over 68 million tons of goods transported by sea each year [12]. The Battle of the Atlantic, which lasted from 1939 to 1945, was a prolonged naval campaign where the Allied forces sought to protect merchant ships carrying essential supplies from North America to Britain and the Soviet Union. German submarines, aware of this British vulnerability, positioned themselves to inflict maximal disruption by sinking these ships. The German submarine commander's assertion that the most important strategic task was the tonnage warfare against British merchant ships reflected a grim reality for the British. This disadvantage in resource transportation further pushed the British people to put more effort in breaking the German Naval Enigma, as acquiring German U-boat positions and movements was crucial for ensuring the safe passage of convoys and maintaining the flow of wartime supplies.

3. Challenges of Decrypting the German Naval Enigma

In contrast to the German Army Enigma, the Naval Enigma posed greater challenges due to its advanced encryption features. Notably, it incorporated three additional scramblers and allowed operators to adjust the reflector to one of 26 orientations. Moreover, Naval operators eschewed stereotypical messages, minimizing opportunities for cryptanalysis and complicating decryption efforts. Unlike German Army, the Naval operators avoided using stereotypical messages, such as "good morning," "RAF plane over airport," or "nothing to post." The disappearance of these frequently used phrases, or cribs, caused consequential setbacks in the efficiency of the British since it relied on reliable cribs to decrypt German codes, significantly reducing opportunities for cryptanalysis and making it unclear where to begin the decryption process [9].

The work of decrypting the German Naval Enigma in 1940, while promising, fell short of expectations. The troubling process began with the initial attempt of the first Bombe Machine, named Victory, at Bletchley Park in March 1940. British codebreakers considered Victory inadequate as it was significantly slower than anticipated, taking up to a week to decipher a single key [13]. Such ineffective decryption process was incomparable to Germany's progress in both updating Enigma key and bolstering defensive ability. Additionally, the Germans captured the British Navy's "Merchant Ship Confidential" along with several cipher tables at the beginning of World War II. This enabled the German Navy to track the movements of Allied merchant ships, enhancing the power and accuracy of submarine attacks and positioning the Allies at a disadvantage due to the time wasted in void decryption efforts [14]. The Allies also faced setbacks, such as a key exchange protocol change by the Germans on May 1, 1940, which invalidated all previous Allied efforts, forcing them to start from scratch and necessitating a reset of decryption efforts and complicating the deciphering process.

In the first few months of 1940, the Allies naturally resumed technological decryption, which had previously led to enormous successes. Despite the British codebreakers' fruitless attempts to obtain enemy military secrets and the exposure of British codes allowing Germans to locate them, merely half a year of failure could never overshadow a decade of pride in smooth decryption. It was conceivable for them to proceed by improving their decrypting machinery, maintaining the optimism their past successes had given them. However, within three months, they once again encountered adversity, dissipating the effort British codebreakers had put in over the half-year period.

The Allies struggled to obtain any useful information through manual decryption until the production of an enhanced Bombe, Agnus Dei, on August 8. Despite significant improvements in decryption technology, the initial months following the employment of Agnus Dei were still filled with obstacles and stagnancy. To crack the Naval Enigma code by decryption, the first critical step was obtaining a "crib," a plausible guess of what a segment of the encrypted message might contain. This guess was essential for setting the Bombe's initial configuration. Then, the British codebreakers could continue to investigate probable correspondence between plaintext and cipher text by ruling out the possibility of having a letter to be identical before and after encipherment [11]. However, even with a potential crib, British codebreakers lacked interpretation certainty, compounded by challenges in accurately positioning the crib within the ciphertext. Cryptanalysts often faced the challenge of correctly aligning their guessed phrase with the corresponding encrypted text [15].

As the Battle of the Atlantic raged, British success against German U-boats remained frustratingly out of reach, with the German submarines' locations shrouded in mystery to the British Operational Intelligence Centre. The complexity of the "Enigma code" utilized by the German navy presented an insurmountable challenge that government cipher schools were initially unable to meet [16]. This uncertainty underscored the critical need for innovation in intelligence-gathering methods. While politicians at the time fully recognized this time-consuming need for intelligence-upgrade, they needed a much more urgent solution that could turn the tide quickly amid the raging war.

4. The Shift towards Stealing Enigma Materials

Faced with this imperative, British codebreakers demonstrated outstanding ingenuity. Arguing that necessity is the mother of invention, they, after seven months of fruitless efforts to decipher the German Naval Enigma, devised a bold and unorthodox strategy. This plan was detailed by British Lieutenant Commander Ian Fleming in a succinct letter dated September 4th, 1940 [17]. This strategy involved using a German bomber to feign distress after an overnight bombing mission. The plan called for the bomber to simulate engine failure over the English Channel, emit smoke, and transmit a distress signal before making a controlled crash into the sea, where the crew, awaiting rescue by a German naval vessel, would seize it to capture Enigma materials [18]. Despite its ingenuity, the strategy ultimately failed due to the absence of German naval vessels to enact the final part of the plan.

A key distinction between stealing and technologically decrypting the Enigma key lies in their pace of progress. Technological decryption, akin to constructing a skyscraper, advances incrementally and at an uncertain speed. In this analogy, "cribs" act as the building blocks, while the Bombe functions like construction equipment, such as an elevator. Without these blocks, decryption cannot proceed, compelling codebreakers to investigate the intricate cipher patterns — the "clay"— to create them. Decryption efforts reset completely when Germany alters its Enigma key. In contrast, stealing can deliver an immediate outcome. It is a binary event that either completely fails or achieves a direct success, akin to hijacking the entire skyscraper. A successful stealing of important Enigma materials, including daily rotor positions, ring settings, and cross-pluggings from the boat would grant the British access to the most advanced Naval code keys and lay the groundwork for facilitating decryption of future German military communications [19]. A success in stealing the Enigma key demonstrates that while manual decryption relies on obtaining cribs for each month's Enigma key, stealing provides direct translation rules for the entire month, to ensure the safe passage of war supplies and materials and significantly reduce war casualties for the Britain. British people could utilize the stolen Enigma key until Germans ultimately change their encryption materials due to safety consideration rather than suspicion about the leak due to their overconfidence in the system's security. Then, the British government could initiate another round of stealing. This effectively cut to minimum the time lag between a German upgrade in encryption and the British decryption effort.

5. Successful Enigma Material Thefts and Their Impact

5.1. The Lofoten Islands Raid (February 1941)

The first notable stealing success from Fleming’s strategy occurred during a British raid in late February 1941 on the Lofoten Islands near Norway. Lieutenant Sir Marshall George Clitheroe Warmington of the Somali opened a wooden box he found on a German ship that had sustained damage in the raid. While the box contained rotors that Hut 8 already possessed, it also held various documents, crucially including the Enigma key tables for February that year [20]. Despite deficiency in quick translation, this Enigma key enabled the Allies to decode all of February's Enigma telegrams in March and March's telegrams by April. The decrypted messages served as valuable cribs, improving the speed and efficiency of translating Naval Enigma codes into actionable military intelligence. This improved efficiency led to the decryption of all April's telegrams by May 10, 1941, at Bletchley Park.

5.2. Capture of German Ships (May 1941)

The second harvest of German Enigma resources by stealing occurred in May 1941. On May 7, 1941, and May 9, 1941, the British Navy consecutively captured the German weather ship München and U-boat U-110, obtaining a weather codebook, a short-signal book, and a naval grid chart [21]. This intelligence coup enabled the government code school to accelerate the decryption process, significantly improving the timeliness of German intelligence interpretation. By May 28, 1941, the time delay dropped down to a mere 34-hour window. Three days later, it further decreased to less

than five hours [14]. From June 1940 to June 1941, the German Navy had sunk approximately 50 British convoy ships each month [22]. Specifically, 142 British merchant ships were sunk from March to May of 1941 alone [8]. However, with the time-efficient codebreaking capability in June as a result of stealing, British people could finally react to German military commands with full preparation, marking a temporary end to such disastrous war trend in 1941.

5.3. Turning the Tide of the Battle of the Atlantic

The efficient Enigma cipher interpretation provided accurate insights into German military arrangement, enabling British merchant ships to navigate safer routes for resource transportation. British codebreaking efforts facilitated the creation of a map (reproduced in **Figure 1**) of the Atlantic Ocean on October 15, 1941, pinpointing accurate German U-boat locations, including Wolfpack, Bismarck, and others. With location markers, British merchant ships evaded all U-boat patrols in the center of the Atlantic Ocean by navigating northern or southern detours toward the U.S. [23].

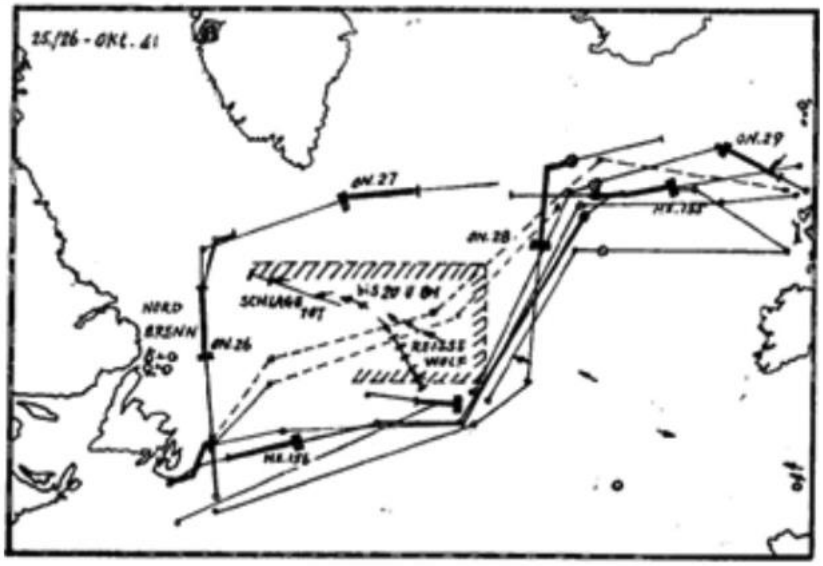


Figure 1. Map of the Situation of Submarines and Convoys in the North Atlantic on October 25 and 26, 1941.

6. Moral Considerations: Stealing vs. Decryption

6.1. Utilitarian Perspective: Focus on Consequences

Moral issues regarding stealing and decrypting the Enigma key are also worth debating. Although theft initially sounds more unethical than decryption, both modes of operation aim to perform the same task: to break into German military secrets and cause similar consequences. Some people may argue that these two approaches end up with different levels of accomplishment. Particularly, technological decryption relies on constantly gaining cribs, so the information acquired remains partial. In contrast, stealing the Enigma key accurately interprets all ciphertexts since, if the British Navy adjusts the rotors correctly, all ciphers convert to plaintext. However, from a utilitarian perspective, as long as both methods aim to obtain German military secrets for military necessity and defensive considerations, they are morally equivalent since utilitarianism focuses solely on the consequences.

We can draw an analogy between the decision-making in this event and the famous Trolley Dilemma, where a bystander could either choose to do nothing and have the train murder five people tied to the track or press down the switch intentionally to redirect the train and kill one person tied to the other track. According to a survey involving numerous philosophers across age, gender, and nationality,

68.2 percent of the philosophers agreed to switch, whereas only 7.6 percent of those philosophers agreed to not switch, thus killing the five instead of one [24].

6.2. The Trolley Dilemma Analogy

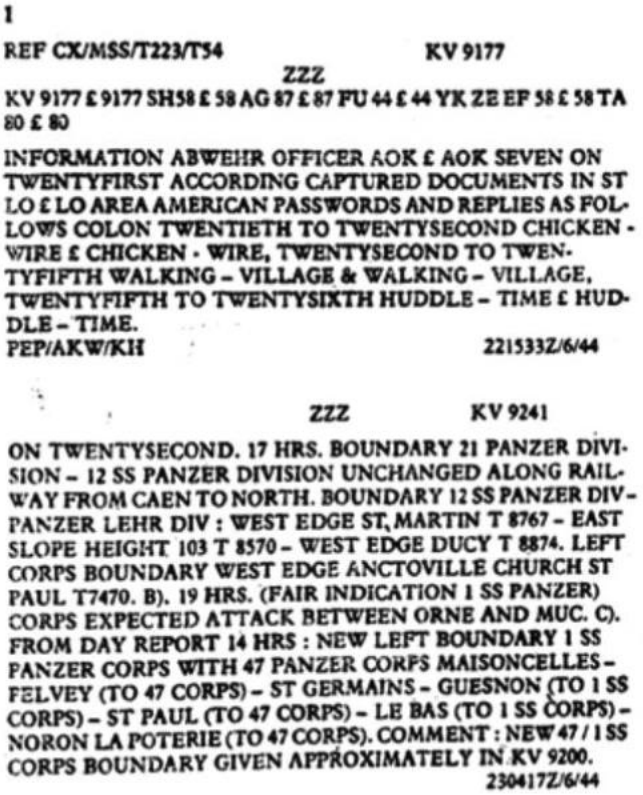
Integrating the conceptual terminologies from Katherine Kortenkamp's research, almost ten times as many philosophers chose to practice utilitarian judgment by saving five people and killing one. The utilitarian judgement in this scenario singularly defines the benefit of the action as a life saved, with no regard to the person being saved per se. This type of judgement weighed the costs and benefits of the action and finally settled on the choice that generates the highest benefit-to-cost ratio, which is the highest effective number of lives saved [25]. With this utilitarian framework, we can justify stealing and consider it a moral action for the British government. We can reasonably assume that the number of lives directly and indirectly saved by successfully stealing Enigma materials, which was in the millions, far outweighed the number of lives lost in stealing operations, which historians did not report but estimated to be in the range of hundreds. The crew stealing the Enigma had a decent chance of returning successfully with German Naval Enigma with no major harm or losses. In The Code Book, Simon Singh mentioned the British Intelligence "assembled an aircrew of German-speaking Englishmen," indicating a careful selection of the most suitable and prepared members [26]. The cost to benefit ratio in this lives-risked-again-lives-saved calculation would be immeasurable, justifying the morality for stealing.

6.3. Deontological Justification for Stealing

Furthermore, factors in the plan for stealing the Enigma key align with deontological judgment, mitigating objections against intentional harm. While the intention of the Germans was to sink British ships, directly contributing to casualties, the intention of stealing was to reduce these casualties. The deontology morality framework aligns with people’s universal morals rules, such as “don’t kill.” Hence, from a deontological perspective, the British government had moral justification in stealing Enigma materials to actively reduce the number of lives lost in the war. Considering both the substantial benefits and the non-violent nature of this action, the justification for stealing the German Enigma key becomes more compelling.

7. Resource Comparison: Decryption vs. Stealing

During 1940 and 1941, not only were pure decryptions ineffective and less ethically compelling to stealing the German Naval Enigma key, but these efforts also required significant human and technological resources. Bletchley Park, at the start of the Battle of the Atlantic in 1939, employed 200 workers, a number that surged to over ten thousand by the end of 1945 due to the critical demand for codebreaking labor [27]. While not all staff members were directly involved in decrypting the German Naval Enigma, they contributed to delivering codebreaking achievements to the British Naval Operational Intelligence Center. However, challenges persisted, with translation errors leading to fragmented information in decoded German Naval Intelligence. A photo from June 1944 (see **Figure 2**), showing two interpreted pieces of German Naval Intelligence, illustrates that much of the information remained fragmented, presenting data such as time, U-boat names, and notable leaders in a disjointed arrangement [28]. This indicated that when British Naval codebreakers struggled to fully interpret the German Naval Enigma, Hut 3 at Bletchley Park had to consolidate all other potential telegrams from the Army and Air Force, annotating them thoroughly before forwarding to the Naval Operational Intelligence Center to enhance understanding of German naval strategies.



1

REF CX/MSS/T223/T54 KV 9177

ZZZ

KV 9177 £ 9177 SH58 £ 58 AG 87 £ 87 FU 44 £ 44 YK ZE EF 58 £ 58 TA 80 £ 80

INFORMATION ABWEHR OFFICER AOK £ AOK SEVEN ON TWENTYFIRST ACCORDING CAPTURED DOCUMENTS IN ST LO £ LO AREA AMERICAN PASSWORDS AND REPLIES AS FOLLOWS COLON TWENTIETH TO TWENTYSECOND CHICKEN - WIRE £ CHICKEN - WIRE, TWENTYSECOND TO TWENTYFIFTH WALKING – VILLAGE & WALKING – VILLAGE, TWENTYFIFTH TO TWENTYSIXTH HUDDLE – TIME £ HUDDLE – TIME.

PEP/AKW/KH 221533Z/6/44

ZZZ KV 9241

ON TWENTYSECOND. 17 HRS. BOUNDARY 21 PANZER DIVISION – 12 SS PANZER DIVISION UNCHANGED ALONG RAILWAY FROM CAEN TO NORTH. BOUNDARY 12 SS PANZER DIV – PANZER LEHR DIV : WEST EDGE ST. MARTIN T 8767 – EAST SLOPE HEIGHT 103 T 8570 – WEST EDGE DUCY T 8874. LEFT CORPS BOUNDARY WEST EDGE ANCTOVILLE CHURCH ST PAUL T7470. B). 19 HRS. (FAIR INDICATION 1 SS PANZER) CORPS EXPECTED ATTACK BETWEEN ORNE AND MUC. C). FROM DAY REPORT 14 HRS : NEW LEFT BOUNDARY 1 SS PANZER CORPS WITH 47 PANZER CORPS MAISONCELLES – FELVEY (TO 47 CORPS) – ST GERMAINS – GUESNON (TO 1 SS CORPS) – ST PAUL (TO 47 CORPS) – LE BAS (TO 1 SS CORPS) – NORON LA POTERIE (TO 47 CORPS). COMMENT : NEW 47 / 1 SS CORPS BOUNDARY GIVEN APPROXIMATELY IN KV 9200.

230417Z/6/44

Figure 2. This file photo shows two examples from the Normandy landings. The decrypted information from the Normandy Landing proves the scatteredness of Naval military communication and is only valuable when incorporating several intelligence and telegrams from both army and air forces.

7.1. Challenges in Decryption Efforts

The high demand for human labor in German Naval Enigma decryption also led to various challenges, further delaying codebreaking progress. This could be exemplified by the fear of advertising or communicating when experiencing a lack of workers. Even British Prime Minister Winston Churchill's visit on September 6, 1941, failed to address the staffing shortage due to hesitation among codebreakers to directly inform him [29]. The Director of Bletchley, Edward Travis, blocked efforts to hire more people, citing an inability to justify additional resources. These challenges prolonged the decryption efforts, allowing German B-Dienst to exploit Allied vulnerabilities and crack their codes [30].

7.2. Cost-Effectiveness of Stealing

Compared to the substantial resources needed for decryption, stealing the Enigma key required far fewer, relying more heavily on luck and chance. Ian Fleming’s plan, for instance, simply involved a group of German-speaking Englishmen with a malfunctioning engine, leaving the timing of an attack to pure chance [21]. Another method of stealing involved using British destroyers to attack a targeted German U-boat, exemplified by the attack on U-110 on May 9, 1941 [31]. All British people needed was a small crew and either an accurate estimation of the target's location or good fortune. Thus, neither approach of stealing was likely to face resource constraints, making it a more cost-effective strategy than pure decryption.

8. Conclusion

The evaluation of stealing and decrypting the German Naval Enigma key during the Battle of the Atlantic from 1940 to 1941 reveals both the complexities and ethical considerations in intelligence

operations during war time. Throughout this period, British efforts to gain access to German Naval Enigma materials through both technological decryption and strategic theft exemplified the ingenuity and resourcefulness of Allied codebreakers. While decryption efforts faced significant challenges, such as the complexity of the Enigma cipher, continuous evolution of German encryption methods, and shortage of staffing, stealing the Enigma key offered a more effective, cost-efficient, and impactful outcome. Despite initial setbacks, successful stealing attempts provided the Allies with invaluable insights into German naval operations, significantly enhancing their ability to respond to U-boat threats in the Atlantic.

From both utilitarian and deontological perspectives, the act of stealing is not only morally justified but most likely superior to technological decryption. Drawing parallels to ethical frameworks such as utilitarianism and deontology, it becomes evident that the perceived benefits of stealing, for instance, the potential to save lives and gain strategic advantages, outweighed the ethical concerns associated with covert operations. There is an intimate connection between strategy, ethics, and technological innovation in wartime intelligence operations, underscoring the necessity for well-balanced decision-making and adaptability in the face of evolving threats when traditional decryption methods failed to work, while also emphasizing the enduring legacy of Allied efforts to unravel the mysteries of the Enigma Machine during World War II.

References

[1] G. Bateman, The Enigma Cipher Machine, American Intelligence Journal 5 (1983) 6-7.

[2] R.A. Ratcliff, How statistics led the Germans to believe Enigma secure and why they were wrong: Neglecting the practical mathematics of cipher machines, Cryptologia 27(2) (2003) 119-131.

[3] J. Wilcox, Solving the Enigma History of the Cryptanalytic Bombe, National Security Agency, Fort George G. Meade, Md, 2006, pp. 7-18.

[4] K. Gaj, A. Orłowski, Facts and Myths of Enigma: Breaking Stereotypes, in: Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2003, pp. 106-122, 110-111.

[5] D. Kahn, Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects, The Historical Journal 23(3) (1980) 629-639.

[6] G.M. Bateman, The Enigma Cipher Machine, American Intelligence Journal 5 (1983) 7.

[7] D. Kahn, Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects, The Historical Journal 23(3) (1980) 629.

[8] S. Gao, Er zhan zhong de mi ma zhan [The Code War in World War II], China Academic Journal Electronic Publishing House, Beijing, n.d.

[9] S. Singh, The Code Book: The Science of Secrecy from Egypt to Quantum Cryptography, first ed., Anchor Books, New York, 2000.

[10] R.A. Ratcliff, How Statistics Led the Germans to Believe Enigma Secure and Why they were Wrong: Neglecting the Practical Mathematics of Cipher Machines, Cryptologia 27(2) (2003) 119-131.

[11] D.W. Davies, The Bombe: A Remarkable Logic Machine, Cryptologia 23(2) (1999) 108-138.

[12] Z. Liu, Di er ci shi jie da zhan qing bao shi [History of World War II Intelligence], Jie fang jun chu ban she, Beijing, 2009, p. 189.

[13] S. Singh, The Code Book: The Science of Secrecy from Egypt to Quantum Cryptography, first ed., Anchor Books, New York, 2000, pp. 176-177.

[14] Z. Liu, Di er ci shi jie da zhan qing bao shi [History of World War II Intelligence], Jie fang jun chu ban she, Beijing, 2009, p. 190.

[15] S. Singh, The Code Book: The Science of Secrecy from Egypt to Quantum Cryptography, first ed., Anchor Books, New York, 2000, p. 177.

[16] Z. Liu, Di er ci shi jie da zhan qing bao shi [History of World War II Intelligence], Jie fang jun chu ban she, Beijing, 2009, p. 193.

[17] S. Budiansky, Battle of Wits: The Complete Story of Codebreaking in World War II, Simon & Schuster, New York, 2000, p. 158.

[18] S. Budiansky, Battle of Wits: The Complete Story of Codebreaking in World War II, Simon & Schuster, New York, 2000, pp. 158-159.

[19] H. Hinsley, A. Stripp, Codebreakers: The Inside Story of Bletchley Park, first ed., Oxford University Press, Oxford, 2001, pp. 122-123.

[20] J. Richelson, A Century of Spies: Intelligence in the Twentieth Century, Oxford University Press, New York, 1995, p. 192.

[21] Z. Liu, Di er ci shi jie da zhan qing bao shi [History of World War II Intelligence], Jie fang jun chu ban she, Beijing, 2009, p. 193.

[22] S. Singh, The Code Book: The Science of Secrecy from Egypt to Quantum Cryptography, first ed., Anchor Books, New York, 2000, p. 182.

[23] L. Wu, Mi ma yu zhan zheng: Wuxian dian zhen cha ji qi zai di er ci shi jie da zhan Zhong de zuo yong [Cipher and War: Radio Reconnaissance and Its Role in World War II], Qun Zhong chu ban she, Beijing, 1984, p. 147.

[24] D. Chalmers, What Do Philosophers Believe, Springer Science, New York, 2013, p. 16.

[25] K. Kortenkamp, Ethics under Uncertainty: The Morality and Appropriateness of Utilitarianism When Outcomes Are Uncertain, The American Journal of Psychology 127(3) (2014) 367-368.

[26] S. Singh, The Code Book: The Science of Secrecy from Egypt to Quantum Cryptography, first ed., Anchor Books, New York, 2000, p. 183.

[27] M. Wu, En ni ge ma mi ma ji yin fa de gu shi er zhan zhong mi ma dui lei zhan ji shi [The Enigma Cipher Machine: A Chronicle of Cryptographic Battles in World War II], China Academic Journal Electronic Publishing House, Beijing, n.d., p. 13.

[28] L. Wu, Mi ma yu zhan zheng: Wuxian dian zhen cha ji qi zai di er ci shi jie da zhan Zhong de zuo yong [Cipher and War: Radio Reconnaissance and Its Role in World War II], Qun Zhong chu ban she, Beijing, 1984, p. 83.

[29] S. Singh, The Code Book: The Science of Secrecy from Egypt to Quantum Cryptography, first ed., Anchor Books, New York, 2000, p. 178.

[30] S. Singh, The Code Book: The Science of Secrecy from Egypt to Quantum Cryptography, first ed., Anchor Books, New York, 2000, p. 179.

[31] J. Richelson, A Century of Spies: Intelligence in the Twentieth Century, Oxford University Press, New York, 1995, p. 193.