H-Net Reviews
in the Humanities & Social Sciences

Rebecca A. Ratcliff. *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers.* New York: Cambridge University Press, 2006. xvii + 314 pp. $30.00 (cloth), ISBN 978-0-521-85522-8.

Reviewed by Katrin Paehler (Department of History, Illinois State University)

Published on H-German (May, 2007)

Of Trees and Forests: Signal Intelligence in World War II

Who would have guessed that signal intelligence could make such a riveting read! To be sure, the tale of the Enigma machine, its German developers' firm belief that the code could not be broken, and its code-breakers is a fascinating story. In the hands of a lesser scholar and writer than Rebecca Ratcliff, however, this study might have been one through which only experts could trudge. Instead, Ratcliff delivers a brilliantly clear historical investigation of German and Allied signal intelligence and their structural and cultural possibilities and limitations. The book not only amazes the expert, but is eminently readable for anyone interested in matters of intelligence, past and present. Ratcliff's excellent study might even work in an undergraduate classroom, as the book takes on a decidedly "sexy" topic likely to strike students' fancy and hold their attention while imparting much broader insights.

By now, the *Reader's Digest* version of the story is well known: National Socialist Germany relied on the Enigma, an electro-mechanical enciphering machine, to encode all its radio traffic. The machine was widely regarded as statistically unbreakable; experts in Germany never seriously considered the notion that their codes could, indeed, be cracked. However, British cryptanalysis did exactly that with information from prewar Polish cryptographers, thereby providing Allied military commanders with detailed "Ultra Secret" messages that in turn influenced all major battles in the western theater of war. In short: Nazi Germany believed it had an absolutely secure code system and the British broke it, but never showed their cards. In fact, well into the postwar period, former members of Nazi Germany's intelligence complex liked to boast of their impregnable codes. Their bubble burst in 1974 when the British finally confirmed that they broke Enigma during the war.

Ratcliff's study admirably addresses the two main questions arising from this basic narrative. How could the Germans have failed to notice that the enemy was reading their encrypted traffic? How did the Allies manage to break the German codes? Consisting of nine chapters plus an introduction and conclusion, Ratcliff's book approaches these questions straightforwardly and logically. Her initial three chapters discuss the machine and the German organizations that dealt with its security and attacks on enemy systems. The subsequent two chapters turn to the Allied side of the story, focusing on signal intelligence (sigint) endeavors at Bletchley Park and the work done to disguise and disseminate "Ultra Secret" information. The subsequent chapter concentrates on German concerns about Enigma's security and investigations into the possibility that secrets had been betrayed, while the following chapter deals with Allied approaches to security and potential leaks. Chapters 8 and 9 focus on the underlying reasons for the two agencies' different approaches to and organization of intelligence matters, convincingly supporting her argument that Enigma's defeat had little to do with its technological flaws but with the system-level failure of one intelligence system–its structure, operation, and culture, which shaped its employees and their abilities–and, conversely, the consis-

tent success of another.

The first chapter sets up Ratcliff's study perfectly. Having realized that Great Britain had beaten them in the intelligence war during the Great War, the German military decided that it needed to do more than rely on codebooks, which could be captured. They found their deliverance in the electromechanical encryption that the Engima machine, initially developed for commerce, promised. From now on, the German military, and by the beginning of the Second World War, each of its the branches, as well as the police, the railways, and the Nazi Party, basked in a sense of security. Each had at its disposal an individualized variation of a statistically unbreakable, easy-to-use system. Ratcliff does a wonderful job of describing the machine's function, the importance and limitations of its upgrades, German security measures to safeguard it, its day-to-day use, and its resulting vulnerabilities, a function of the constant use of one cryptographic system by German agencies all across the military and political spectrum. Here the author impresses with her clear explanation of technical matters; what could be complicated and cumbersome becomes strikingly clear.

Similarly, Ratcliff's discussion of the German intelligence complex persuades through its straightforward manner. She focuses on several key elements: the German penchant for decentralization and specialization, as well as the tendency to focus on the short-term, instant-gratification tactical signals of the enemy. Nazi Germany did, indeed, secure several offensive successes with tactical intelligence, serving the military commanders of the various branches well, but this focus also increased "segregation and autonomy" and eventually led to serious disadvantages (p. 54). Early successes confirmed to German sigint units that they were doing well, but more importantly, the lack of cooperation also meant that information was not shared, security measures were implemented unevenly, and good cryptanalytic practices were not applied across the board.

Blinded by early successes, the Germans saw little need to change a winning horse. However, the decentralization of the various German intelligence branches in collecting intelligence also led to decentralization of security. Agencies simply did not cooperate. This overall situation was only worsened by competition among the various branches and agencies; any cooperation that did occur was ad hoc and based on personal relationships. Other problems stemmed from this setup. Different agencies competed for a limited number of qualified people, all the while putting a high premium on "origin and background, tradition and social standing" while creating overlaps and redundancies (p. 63). Ratcliff argues interestingly that these flaws cannot be blamed on National Socialism. They came courtesy of the traditional German military mindset and structures, even though the division and competition among the various intelligence branches suited Adolf Hitler. Security could only have been achieved through cooperation, especially in a situation where all agencies shared one encryption system, regardless of the system's apparent security.

In subsequent chapters, Ratcliff turns her attention to the Allied, largely British, side of the story, presenting almost the inverse image of Germany's organizations. British cryptanalysis entered the war woefully underprepared, but with backing from the highest levels of the government, the British began to centralize their intelligence efforts in Bletchley Park and to throw financial and personnel resources at the problem. Three years later, Allied intelligence was cracking and reading Enigma ciphers on an almost daily basis. Ratcliff strongly supports her point that the British were not just lucky, but that they created their own luck over the course of time. High priority was given to cryptanalysis, which is not unusual for a nation on the defensive, and support from the prime minister unlocked much-needed resources.

Most importantly, though, the British dared to think outside the military box. While in Germany intelligence specialists were military men, many seriously disgruntled because intelligence was not considered a military career at all, Britain turned to the great untapped resource of civilians from all walks of life. Military promotions were of little interest to these men and women. The British intelligence community called into service intellectual amateurs, ivory-tower scholars, hot-shot business leaders, chess champions, *Times* crossword puzzle winners, members of the national bridge team, a number of Egyptologists, antiquarian booksellers, and (my personal favorite) porcelain experts. The common denominator that made these people good at code-breaking was their ability "to recognize, categorize, and contextualize unfamiliar material" (p. 80). While not sugarcoating the health and influence of the British old boy network, Ratcliff draws attention to the fact that cryptanalysis also relied on the "great unwashed" if they could be of service: Jews, Muslims, women, German immigrants, communists, and fairly recently naturalized British citizens. Diversity facilitated success.

At Bletchley Park, success was also achieved through

flat hierarchies and excellent military-civilian collaboration. Ratcliff aptly describes the setup as the perfect balance "of military structure and civilian mentality" (p. 82). It appears that these civilian "geeks" quite liked their work, in some cases so much so that they had to be ordered to take days off. Workers at Bletchley Park were informed about the larger issues, understood where their work fit into the big picture, and were schooled in all matters concerning the intelligence war. Open communication led to innumerable successes that could have not been achieved in a compartmentalized, strictly hierarchical system. This integrated system, which contained minimal or no redundancy, made Britain successful. Having recognized that Enigma was a single system of related variations, the British attacked it as a single problem by using and exploiting connections and security violations, eventually with an almost shocking success rate.

Once Enigma's security was breached, the British intelligence complex did not rest on its laurels, but added to them, Ratcliff asserts, through the "near perfect security which surrounded the deciphering effort" (p. 106). As with the decryption, successful implementation of security was a function of centralization and the almost counterintuitive willingness to share high-level information if it allowed an individual to do his or her job better and prevented unintentional slippage. Security is achieved more easily when the height of the stakes is known and appreciated. Distrust also helped: while the British were often wearied by American laxness, still British and American officials agreed that other Allies could not be trusted by a long shot. In addition, elaborate cover stories, such as the famous, but entirely fictitious highly-placed German agent "Boniface" were created, and Ultra intelligence (the term for the harvest of Enigma-encoded dispatches) was used as a guide for confirming and exploiting low grade intelligence rather than a source of such information in its own right. The Allies also used Ultra intelligence to feed red herrings to the Germans; for example, by drawing German attention to completely imaginary Italian agents. In addition, Allied intelligence did everything it could to avoid the German mistakes that had allowed them to break Enigma in the first place. Paraphrasing can go a long way to boosting signal security, as can separate signal networks and Special Liaisons Units.

In chapter 6, Ratcliff returns her attention to the German side of the story. The German military knew that something was up; Allied intelligence was just too good to be true. Using a number of German investigations as case studies, Ratcliff shows how, despite evidence to the contrary, German investigators in nearly every branch of the military managed to find alternate explanations for surprising Allied knowledge. The lack of German interagency cooperation only compounded the problem; the possibility that a systemic problem existed did not register. German investigations read, to some extent, like comedies of errors. For example, German investigators argued that an intercepted Allied message was not based on Enigma because it was not a word-for-word translation of the original massage. The fundamental source of these problems, however, is found in the German conviction that Enigma was statistically unbreakable. Rather than setting out to prove that Enigma might have been broken, German investigations set out to prove, sometimes through tenuous logic, that Enigma could not be at fault. Looking at the trees, the Germans missed the forest.

The Germans were assumed that Enigma could only be broken through physical assault, and not through analysis. Consequently, German investigators concluded that the enemy would either be able to read all the ciphers or none at all, thereby completely discounting the possibility of what was actually happening: constant, if sometimes partial reading with a short time delay, as the British had to reconstruct the code key every day. German belief in Enigma held firm, even after Swiss informant gave notice that Americans were reading Enigma traffic concerning submarines. This knowledge did not raise too much alarm in Germany, as it was assumed that the enemy had in possession at most the Enigma keys for a particular month, which would expire eventually.

In her explanation of the German unwillingness to consider the obvious, Ratcliff points at an interesting cultural issue: German officers and cryptologists considered "cryptology and ciphers an intellectual invention rather than a mechanical one" (p. 156). The Germans believed that the Allies, especially the British, had hung the moon when it came to mechanical inventions like radar, but were not intellectuals. The Germans were intellectuals and thus assumed that the British could not have broken Enigma.

In providing security for their own signal intelligence, the British took the opposite approach. Rather than resting after their success in breaking Enigma, they read it as a warning of the impossibility of full security. Consequently, the Allies embraced a constant level of alert, perpetually testing machines and improving security for signal intelligence. This activity included Allied attempts to identify and fix problems within their own

systems, but even more importantly, they were willing to draw undesirable conclusions and take (sometimes very expensive) action, such as replacing major machine components worldwide to prevent German breakage of Allied codes. In the end, the efforts paid off. All Allied high-grade security systems survived the war intact.

In chapters 8 and 9, Ratcliff focuses on explanations for German failures and Allied successes, drawing together the insights from her preceding chapters. Most importantly, she argues that the reasons for German failures were German and not National Socialist, even though she alludes to the exacerbation of systemic and cultural problems prevalent in the German military under the Nazi regime. The German military had always focused on tactical intelligence, limited resources for intelligence efforts, and restricted its pool of applicants through "rigid hiring practices, which emphasized military loyalty, racial and social heritage, seniority, and class, rather than aptitude, skills, and proven track record" (p. 192). While lack of cooperation as a feature of the German intelligence complex preceded the Nazis, under them it worsened; "[n]one of the German sigint bureaus recognized the lurking disaster of pairing cryptographic cooperation via Enigma with compartmentalization in cryptanalysis and security" (p. 187). In addition, intelligence was low on everybody's list of priorities. Hitler relied on his "military genius," while Wehrmacht officers were dealing with the demands of a multiple-front war. The dearth of cooperation made the lack of men and materiel in Germany even more strongly felt. Funding and qualified personnel were hard to come by and sometimes, as in 1944, intelligence personnel found themselves harvesting potatoes (p. 190). The lack of priority and prestige ascribed to intelligence also translated into a lack of importance; intelligence was not taken seriously.

Finally, the German intelligence community failed to notice that cryptology was coming of age. Cryptography had become highly mechanized after the Great War; Enigma was an obvious example. Shortly afterwards, cryptanalysis followed this trend and developed into its own science, ultimately creating the field of computer science. The German intelligence community, having adopted Enigma, missed the analogous change in cryptanalysis. In contrast to their British counterparts, the German intelligence community did not rely on academics; little contact and cooperation took place between the military and scientists, exceptions such as the rocket program notwithstanding. This issue, too, is largely cultural, according to Ratcliff: German academics were suspicious of the practical applications of their work. Similar cultural issues were at work with members of the German intelligence community. The few tools brought in to help with cryptanalysis were frequently and derisively referred to as "gadgets," implying a level of charlatanic wheeling and dealing. The German military saw cryptanalysis idealistically, as "mental work" (*geistige Arbeit*), in which using "gadgets" was cheating (p. 211). In the end, Germany found itself trapped in a paradox: it had made a tremendous leap forward with the initial adoption of Enigma, but then stood still in cryptanalysis, stubbornly relying on the belief that codes created by machines such as Enigma could not be broken. Thus the Germans did not even try to break the codes of similar Allied machines.

In addition to summarizing her findings regarding Germany and discussing the reasons for British success as the inverse of German failure, Ratliff's conclusion draws well-conceived lessons with obvious applications for our technological present and future. Where Germany lacked resources or prevented itself from tapping them, the Allies made resources available and dared to think beyond accepted norms. While Nazi Germany was defined by a "pervasive culture of self-censorship" (p. 221), decentralization, lack of cooperation, and groupthink, which did not allow for the most logical conclusion–that Enigma had, indeed, been compromised–the Allies created an organizational structure and culture that allowed analysts to see the big picture, gave them autonomy, and made the task at hand more important than "hierarchical and personal concerns" (p. 230). At the same time, the Allies made the protection of Ultra paramount, granting no exceptions at all. While the Germans assumed with an air of superiority that Enigma had solved all their problems, the Allies assumed that the enemy might be smart as well and that even the most sophisticated system could be broken "given enough time, resources, and ingenuity" (p. 233). Ratcliff thus concludes that technological security "was a myth in 1939 and remains a myth in the twenty-first century" (p. 235). She also concludes that the key to Allied success in World War II is found in diversity, the belief in the possible, and the cooperative and collaborative atmosphere of broadly focused organizations that allowed for the recognition of mistakes and their correction. As Ratcliff states so succinctly, "[t]ruly innovative organizations will only emerge in a society that fosters the values of cooperation and problem solving and encourages flexibility, diversity, and innovation" (p. 236).

Ratcliff has written a fabulous book. It is well-

researched, well-argued, and beautifully written. I sincerely hope that it will find a wide array of readers from all walks of academic and non-academic life. It holds insights and lessons aplenty.

If there is additional discussion of this review, you may access it through the network, at:

https://networks.h-net.org/h-german

Citation: Katrin Paehler. Review of Ratcliff, Rebecca A., *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers*. H-German, H-Net Reviews. May, 2007.

URL: http://www.h-net.org/reviews/showrev.php?id=13210