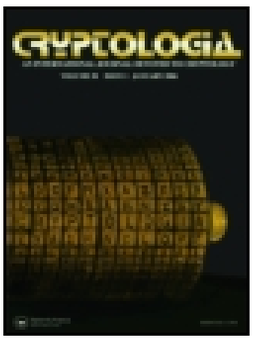

CRYPTOLOGIA

ISSN: 0161-1194 (Print) 1558-1586 (Online) Journal homepage: https://www.tandfonline.com/loi/ucry20

WHY GERMANY LOST THE CODE WAR

DAVID KAHN

To cite this article: DAVID KAHN (1982) WHY GERMANY LOST THE CODE WAR, CRYPTOLOGIA, 6:1, 26-31, DOI: 10.1080/0161-118291856759

To link to this article: https://doi.org/10.1080/0161-118291856759

Published online: 04 Jun 2010.

WHY GERMANY LOST THE CODE WAR

DAVID KAHN

This paper was presented for discussion at the Baltimore-Washington German History Seminar, 8 November 1980, Towson State University, Towson, Maryland. It is a slightly revised form of a portion of "Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects," The Historical Journal, 23 (September, 1980), 617-639, which lists all sources. The technical reasons given below owe a great deal to the kind help of Dr. Cipher A. Deavours.

A spate of books, articles and reports at historical conferences has made it widely known that the Allies solved the high-level German cipher machine called Enigma during World War II. The Germans, on the other hand, did not solve the equivalent Allied cryptosystems, with the exception of Royal Navy codes up to about 1943. The Allies thus had considerable insight into enemy plans and capabilities which the Germans did not have, and these insights greatly contributed to the Allied victory.

Why were the Allies -- meaning the western Allies -- so much better than the Germans in this field, which proved so important? In investigating this question, we might begin by clearing away two theories that at first seem plausible but do not in fact apply.

One is that German codebreakers were chosen for their political reliability as good Nazis instead of for their ability. This did not happen with the German cryptanalytic agencies. The civilian technical heads of the agencies of the navy and of the Oberkommando der Wehrmacht were not members; indeed, the navy man even ousted an Alte Kaempfer in gaining his post. (The military chiefs, who were mainly administrator, were, like all professional soldiers, ineligible to join until 1944.) Of the administrative chief and the three head cryptanalysts of the Foreign Office agency, all of whom held their posts from the 1920s to 1945, none were convinced enough Nazis to have joined before Hitler's accession to power; one never did join and the times of joining of the other three suggest motives other than belief for their doing so; one became a member soon after the Machtergreifung and two during the war. The leading officials of the Forschungsamt, Goering's wiretapping and codebreaking agency, were, on the other hand, all Nazis. Whether the high-ranking civilians in the army and air force codebreaking agencies were party members is not known. Overall, the pattern does not suggest that insistence on party adherence as essential for advancement, but the contrary.

The other false theory is that the Allies were quantum steps ahead of the Germans in cryptology. They were not. Certainly they were more advanced, but the Germans knew the answer to the basic question; how to solve the Enigma. Early in the 1930s, the head cryptanalyst of the Forschungsamt

said to the head evaluator; ''Seifert, die ganze Enigma ist Mist!'' And he proceeded to demonstrate a solution using alphabet slides that was also known -- at least later -- to the Allies. Though a modification (the plugboard) vitiated this technique, the German cryptographers always claimed that the machine was not absolutely secure and continually suggested improvements -- implying that they could see ways of breaking into the machine. So the theory that the Allies knew how to solve the Enigma and the Germans did not is false and not a factor in the Allied cryptologic superiority.

Separate form these theories lies a hypothesis that appears likely but for which proof is lacking. This is that the Allies' larger population gave them more, and probably also better, people for codebreaking than Germany. But it is not known how many of the approximately 10,000 people at Bletchley, as Britain's codebreaking agency was generally called from its location in that town 50 miles northwest of London, were solving ciphers other than German at any particular time, or how many in the German agencies were solving Soviet, Italian, Japanese, Turkish, Swedish, and other non-U.S. and non-U.K. systems at the same time. Moreover, the contributions of other governments -- Canadian, Free French, Dutch, Italian, Japanese, Hungarian -- to their respective allies cannot readily be measured in terms of manpower. Finally, the number of persons in field units, both Allied and German, is not known with precision. Still, it seems probable that more people in the West attacked German ciphers than worked in Germany on Allied ciphers and so greater Allied population probably did contribute to greater success. But, without the data that would prove or disprove this conjecture, it cannot legitimately be advanced. A corollary to this theory would be that the Allies' greater industrial capacity enabled them to help both their codebreakers and their codemakers more. But this help would have been so small in relation to either the Allied or the Axis war effort as to be insignificant. So this cannot be adduced as a factor, either.

What, then, are the factors that led to Allied superiority and German inferiority in codebreaking? There are, of course, a variety of causes for so complex a phenomenon. They may be divided into two kinds -- general and technical. There are four of the latter, all of which spring from purely cryptologic roots.

The first chronologically, and probably also the first in order of importance, is that the Allies knew the fundamentals of the German machine. The Enigma, which had been invented shortly after World War I by a private individual, was offered for sale to the public early in the 1920s; the inventor hoped to become rich as businessmen bought his machine to ensure the secrecy of their communications. The Polish, British, French and U.S. codebreaking agencies acquired the advertising brochures, press reports and patents on the Enigma and, at least Poland also obtained a machine. So even though the German navy (the first German government element to use it) modified it for its own use, and even though the army and other agencies of government further varied it for their own use, the Allies had a basic knowledge of the machine. To this must be added the operating instructions of the military version and some actual keys sold to the French by a German working within the German code agencies whom the French recruited as a spy around 1931. Cryptanalytically, all this information gave the Allies a big

head start. It also gave them an enormous psychological advantage. The Germans did not enjoy such benefits. The Allied analogues of the Enigma, Britain's Type-X and the American SIGABA, were developed in secret. Of course, knowledge of a machine is not always essential for its solution. The Americans reconstructed the Japanese PURPLE diplomatic cipher machine without any such assistance. But acquaintance with the machine cannot but help.

The second technical reason is that the Germans mainly used one machine, the Enigma (though they supplemented it with another machine, the Geheimschreiber, later in the war), while the Allies, consisting of many nations, used many. The German use of one machine entailed several effects for the Allies. First of all, they could concentrate relatively more manpower on the problem. Secondly, the single system generated a greater proportion of messages enciphered in it, thereby facilitating its solution. Thirdly, a single system increased Allied incentive, because its solution would yield a greater prize than if it were just one system among many. None of these factors operated for the Germans, and it correspondingly depressed their efforts and results.

A third cryptologic reason is that the main high-level cipher machine of the Americans, at least, the SIGABA, was far better than the Enigma. Both used the same cryptographic principle, that of the rotor, or wired code-wheel, to create an electrical maze that enciphered the letter. The naval Enigma, the best of the German family, came with a set of eight rotors, of which four were inserted into the machine at one time. Gears controlled their stepping. The SIGABA had 15 rotors,10 for creating the electrical maze, five for moving those 10 in a much more irregular way than gears could, thus making solution more difficult. A cryptologist has said that the SIGABA was "a generation ahead" of the Enigma. It was in fact devised a decade after the Enigma, and because the Americans did not begin equipping their army and navy with cipher machines until the late 1930s, they could utilize this more advanced mechanism without losing capital investment. The Germans, who had mechanized a decade earlier, were stuck with an older, weaker machine.

Fourthly, just as the German hardware was poorer, so was their software. Two of their operating procedures proved fatal to many an Enigma cryptogram. One was the flawed keying method used by the Germans before the war and for its first year or so. It required that a three-letter keying group, such as BOL, be repeated; BOLBOL. The Germans probably did this to enable their clerks to decipher a message even if a garble altered one of the six key letters. But the repetition also created a point of entry for cryptanalysts,which the Poles -- who first cracked the machine -- and then the British quickly exploited. This keying method was later changed, but by then Enigma had been solved. The Allies, on the other hand, used far more secure keying systems which obviated this sort of attack. The other dangerous operating procedure was the transmission of messages without padding (meaningless words at the beginning and end) and without bisection (dividing messages in half and putting the second part before the first). Both of these techniques protected against the stereotyped beginnings and endings of messages or the routine whole messages that soldiers persisted in sending. The Allies broke into many a new Enigma key because an isolated outpost continued to transmit "Nichts zu melden" in the new key

just as it had in the old. Allied soldiers likewise often composed, enciphered and transmitted routine messages, especially in the communications to and from convoys. But the Allied use of padding and bisection afforded their plaintexts better protection than German.

Four technical reasons thus played a role in Allied cryptologic success; Allied knowledge of the Enigma compared with German ignorance of Allied machines; the German use of one main machine versus the Allied use of many; a German machine cryptographically poorer than their Allied equivalents; and German operating procedures that were inadequate in contrast to adequate Allied ones. In addition to these, five general reasons contributed to the Allied success. These flowed from external circumstances, or political and social factors.

Perhaps the most important was the fragmentation of German cryptanalysis. The Germans had a great many codebreaking agencies. The Chiffrierabteilung of the OKW, Pers Z of the Foreign Office, and Goering's Forschungsamt competed on the highest level. For a time, the Sicherheitsdienst, the SS's intelligence army, had its own agency. The army, the navy, and the air force each had its own unit, though there was rather more justification for that. But this multiplicity spread the available manpower, which was scarce to begin with, very thin. And it diffused the codebreaking effort. Contrast this with the concentration of effort at Bletchley, Britain's sole codebreaking agency, and with that in America, where the army and navy codebreaking unity worked in the closest cooperation. Of course, there was some cooperation in Germany. But it did not overcome the lethal effects of dispersion, which stemmed from Hitler's assigning duplicate responsibilites to his underlings so that he could retain ultimate control. The charismatic nature of this leadership enabled him to do this in many areas of government. It facilitated his rule -- but it devastated his war effort, including codebreaking.

Also fundamental as a reason for Allied cryptologic superiority was Germany's aggression and the Allies' defensive posture. Behind this lies the fact that intelligence is necessary to the defense, but it is only contingent to the offense. Clausewitz defined the characteristic feature of the defense as "awaiting the blow." An army can await a blow only if it believes that a blow is planned, and such a belief can be created only by information about the enemy. That is why intelligence is essential to the defense, and Poland, France, and England, basically in a defensive stance, cultivated it. The offense, on the other hand, is "complete in itself," Clausewitz said. An attacking army does not even have to know where the enemy force is: it can march about, imposing its will, until it runs into its foe. Such an army will put more of its effort into men, tanks, planes and guns and less into intelligence, one form of which is codebreaking. This Germany did. A number of incidents and conditions demonstrate her relative neglect of intelligence and the corresponding greater attention that the Allies paid to it.

France gained the spy who provided the Allies with vital cryptologic information in large measure because she made a great -- and generally successful -- effort to learn about German rearmament. The Germans, though their spies sometimes delivered useful cryptologic information, never scored a coup like France's -- mainly because they never tried as hard.

Before the outbreak of war, Great Britain had established an Operational Intelligence Centre in the Admiralty and a Joint Intelligence Committee under the chiefs of staff. Germany never took such steps.

The Allies put better men into cryptology than the Germans. Bletchley Park was an unbelievable galaxy of talent. All American recruits were given an IQ test; those who scored the highest were proposed for cryptologic work. This resulted in extraordinarily high brainpower in codebreaking units. The American army agency could have staffed a first-class university in all departments, one of its leaders boasted, with justice. No such recruiting seems to have taken place for German codebreaking. And their agencies, despite individually bright men, did not dazzle as did the Allied units.

German training for cryptanalysis, too, was poorer than the Allies'. The only textbook the Kriegsmarine had was a translation of an elementary French text. Cryptanalysts learned on the job. The United States, on the other hand, had developed its own textbooks and established schools and extension courses to train cryptanalysts. In the same way, the Allied instructions for cipher clerks on how to set up their machines and how to encipher sometimes explained that certain procedures should not be used because they would help the enemy solve the messages. The German instructions never motivated like that.

Furthermore, while the Germans continued using only electromechanical devices for solving ciphers, the Allies added electronic devices. These in effect multiplied the Allies' manpower and enabled them to do far more in a given amount of time, in particular solving cryptograms enciphered in the new Geheimschreiber rapidly enough for them to be of use to the commanders in the field. The cause of this Allied advance seems to have lain in Britain's urgent need for intelligence. In 1940, with invasion still a possiblity, wrote one who was there, "Bletchley foresaw that the enemy could introduce new practices which would require the [existing electromechanical] breaking machinery to be speeded up by one or two orders of magnitude at least." Such high speeds had been attained in the 1930s by a Cambridge physicist, C. E. Wynn-Williams. He had devised an electronic counter to tally electron-particle events that occurred too rapidly for electromechanical counters. Many of Bletchley's staff had come from Cambridge. They thought of his electronic device when they themselves had to create machinery to count very fast. Their ideas culminated in a remarkable device codenamed COLOSSUS, which many historians of technology regard as the first electronic computer and which significantly contributed to Allied success in cryptanalysis. In Germany, despite a computer pioneer's 1940 proposal for an electronic cipher device, which might have suggested the use of electronics in codebreaking to the army's cryptologic authorities, and despite a later naval proposal for an electronic codebreaking mechanism, no agency apparently ever felt the need to build one. And so Germany never took the crucial step to electronics in cryptanalysis.

All these factors suggested a widespread German disregard for codebreaking relative to the Allies, which may be ascribed to German aggression and Allied emphasis on the defensive.

A third general factor was the expulsion of the Jews. The exodus or extermination of a whole people, many of them highly intelligent, cost

German codebreaking -- as it cost German mathematics and German physics -- many brains.

A fourth general reason was luck. Luck helped the Allies more than the Germans. It certainly played a role in the French recruiting of their important spy, and it was luck that a genius, the mathematician Alan Turing, who had an idea that greatly helped Enigma solutions and that the Germans did not have, was a Briton. But this was not as important a factor as the others.

The fifth and last reason for German inferiority is the broadest: a greater reluctance to face reality. It was this reluctance, combined with the lack of irrefutable evidence for enemy cryptanalysis, that largely kept the naval high command from conceding during several investigations that its cipher might have been broken. The officers found it difficult to admit to themselves, to their chiefs, and to Hitler that everything they had said and done was worthless and would have to be redone. The result was disaster. Of course, the Allies, too, were sometimes reluctant to face reality. Conferences on possible compromises of systems sometimes decided, as the Germans did, that none had occurred, largely because the cryptologists did not want to go through all the work of instituting new systems -- devising, manufacturing, and distributing the new machines, training the personnel, and phasing the system into operation with the inevitable blunders that would call down the wrath of admirals and generals. But the conditions under which the Allies worked made it easier for them to confront unpleasant facts. They were less crippled by arrogance than the Germans and so more open to improvement. [For an attempt to trace the historical roots of German arrogance see David Kahn's Hitler's Spies, (New York, 1978), pp. 525-27.] SIGABA's greater strength enabled the Americans to restore security in case of a compromise by simply replacing rotors; the Germans would have had to substitute a whole new system for the Enigma. Competition between Americans and Britains in a joint endeavor helped keep failure from being hidden for very long. Civilian draftees or volunteers headed important sections of codebreaking and intelligence agencies more frequently in Allied forces than in German; because they were less concerned about their military careers than the officers and officials who headed the corresponding German sections, these civilians admitted unpleasant facts to their superiors more readily. For all these reasons, the Allies seem to have faced reality more. When an American cipher machine went astray in France in 1944, the American army code agency worked day and night to rewire the rotors of other machines, thus making the missing machine useless to cryptanalysts. And when the Americans got wind of the German solution of their military attache code, they distributed a new system. So, as one American cryptologist has said, "We never kidded ourselves. The Germans and Japanese did kid themselves."

These, then, are the five external conditions that helped reduce German cryptanalysis to a level inferior to Allied: the fragmentation of the German organization compared to the unity of the Allied; Germany's aggression, which led to a neglect of cryptology, contrasted with the Allied defensive posture, which emphasized intelligence; the expulsion and killing of the Jews; better Allied luck; and greater German reluctance to face reality. When these are joined to the four technical reasons, they help answer why German cryptanalysis was poorer than Allied, and so help explain one of the causes of the defeat of the Third Reich.