The German Cryptologic Effort 1918–1945

Between the two world wars, six major cryptologic services and bureaus evolved within Germany. Three were responsible mainly for foreign diplomatic systems, and the other three—representing each of the branches of the armed services—for exploiting counterpart foreign military systems. Several additional cryptologic organizations were also established to work against systems used, for example, by enemy agents and for enciphering weather traffic. In the area of communications security, five of these six organizations were responsible for designing and testing their own cryptographic systems, and for insuring their security when used by associated armed forces units or by the diplomatic services. All of these agencies and bureaus existed side by side with more or less equal authority. There was no central coordinating point to fuse, evaluate, and report German communications intelligence, or to safeguard overall communications security.

This situation also prevailed for the major portion of World War II. In the autumn of 1944, however, an attempt was made by the German High Command to establish a single cryptologic policy and to invest one of the existing organizations with the responsibility for its implementation. Special emphasis was placed on the authority given this agency to rule upon the security of cryptographic systems for both diplomatic and military use and to control the development and use of cryptanalytic aids and devices. Interdepartmental jealousies, however, were not easily overcome, and it was not possible during the few remaining months of the War to effectively implement this plan.

German Cryptologic Organization, 1918–1938

Cryptologic Bureaus

The three cryptologic bureaus which existed during World War I continued in operation after the Armistice. The responsibilities of these bureaus were clearly defined, and they functioned, so far as can be determined, as the main cryptologic organizations within the German Government until 1933.

The first of these, the Cipher Bureau of the Ministry of Defense, was responsible for working on foreign army cryptographic systems. The second, the Cipher Bureau of the Foreign Office, was assigned foreign diplomatic systems, and the third, the Cipher Bureau of the German Navy, foreign navy systems. All three were also responsible for insuring the security of counterpart German communications.

This discussion of German cryptology is taken mainly from an Armed Forces Security Agency Council (AFSAC) study produced in 1950, entitled: "The Consequences of Lack of Coordination among the German Cryptologic Services." It is presented in *Spectrum* to show the fragmented German cryptologic effort from 1918–1945, and to show problems such an effort fostered and its consequences to the German war effort.

Despite the clearly defined missions of these bureaus, rivalry between the first two began almost immediately after the Armistice. This rivalry began when the Defense Bureau involved itself with diplomatic systems of foreign governments, clearly an area reserved to the Foreign Office's Bureau. Although a number of reasons were given in attempts to justify this encroachment, they did not satisfy the Foreign Office. Nevertheless, the Cipher Bureau of the Ministry of Defense continued to work in the diplomatic area, thus duplicating to a considerable extent the work of the Foreign Office. Intercept stations of both bureaus were assigned diplomatic targets, and tension and rivalry between the two steadily intensified. The Cipher Bureau of the German Navy, however, limited itself strictly to foreign naval traffic, and as such did not encroach upon responsibilities of the other bureaus, nor they on its mission.

Establishment of the Forschungsamt in 1933

In March 1933, a formidable rival to the existing bureaus appeared under the guise of an organization called the *Forschungsamt* (or "Research Bureau"). This organization, founded by Hermann Goering, then Prussian Minister of the Interior, was placed under the Ministry of Air. In reality, though, it had nothing to do with the solution of air systems, but was instead an "information bureau" of the National Socialist Party. Its distinctly political flavor quickly roused the suspicions of the older bureaus, and initial bitterness evolved into intense rivalry. But the *Forschungsamt*, under the personal tutelage of Goering, became, and remained throughout the war, the largest of the cryptologic organizations.

Air Minister Hermann Goering recognized the need for cryptology on a "broad and general basis," but the only communications intelligence he trusted was that of his own organization.

The Army Cryptologic Service

After the Armistice, the Cipher Bureau of the Ministry of Defense was given the responsibility for insuring the security of Germany Army cryptographic systems, and of those used by the small German Air Force. The limitation placed on the size of the Army by the Treaty of Versailles (limiting it to no more than 100,000 men) did not, at first, make this a burden, but the expansion of the Army and Air Force after Hitler came to power soon overtaxed the capabilities of the Defense Bureau, and in 1936 the German Army assumed these cryptologic functions, to the exclusion of the Defense Bureau. A branch within the Signal Group of the General Army Office was established to handle this task.

The growing independence and size of the Army resulted in the formation in 1938 of a new Army cryptologic service, which was also placed within the Signal Group of the General Army Office. Its formation was opposed by the Chief Signal Officer of the German Army, and by leaders of the Cipher Bureau of the Ministry of Defense. This opposition, and growing pains associated with all new organizations, hampered its effectiveness in subsequent years.

The Air Force Cryptologic Service

During the period of rapid expansion of the German Air Force between 1936 and 1939, Air Minister Goering and the Chief Signal Officer of the Air Force ordered the establishment of an Air Force cryptologic organization. Training of its personnel at first was conducted by an established agency, but soon it too went its own way, and close liaison with others in the German cryptologic effort faded away.

Other Cryptologic Efforts

In addition to these six major cryptologic organizations, there were at least four others of lesser significance with specialized tasks. The first of these, the

Radio Defense Corps, was responsible for the identification and "elimination" of enemy radio agents. Another, the Weather Service, involved itself with weather cryptographic systems. A third, the Postal Service, was given the task of monitoring telegraph, telephone, and mail communications. And the fourth, the Propaganda Ministry, was responsible for the interception of foreign radio broadcasts.

The German Cryptologic Organization in World War II

The Struggle for Authority

By the beginning of World War II, Germany had six major cryptologic organizations, each more or less independent of the others. This situation prevailed, to one degree or another, throughout most of the war.

But an attempt was made during the war to place this fragmented effort under one central authority. It evolved from the realization by persons in the German High Command, and in some of the cryptologic organizations as well, of the need for a centralized authority in cryptologic matters, particularly in regard to safeguarding the security of German cryptographic systems and procedures. Attempts were subsequently made to inaugurate an over-all policy, and to establish a central authority, but with only partial success.

The Armed Forces High Command Cryptologic Agency[1] was selected to provide this leadership, and in September 1943 it was ordered that this Agency must be consulted, and approve, proposed introductions of new cryptographic systems by any branch of the armed forces. Also, in August 1944, this Agency was given the responsibility for chairing a working committee responsible for overseeing the testing of all German cryptographic systems. Under the chairmanship of General Gimmler, numerous high-level meetings were held, attended by representatives of all the cryptologic organizations. General Gimmler, however, found it necessary to dilute responsibilities and authority of the working committee, and to assure the cryptologic organizations that their own prerogatives would be respected. In fact, when corresponding with the other cryptologic activities, he found it necessary to allay any apprehensions they may have had of possible infringement on their areas of responsibility, and actually appealed for their cooperation. Apparently he had no authority to compel such cooperation, noting, in one communication, that "The Armed Forces High Command does not contemplate taking away cryptanalysis from authorities which are doing it now, but . . . requests that the results be made accessible to the Armed Forces . . . for its own control cryptanalysis."

[1] This Agency was previously named the Cipher Bureau of the Ministry of Defense.

Hitler didn't like signals intelligence "very much"; rather, he preferred "common sense."

Consequences of the Lack of Coordination

During the war, it was inevitable that this lack of coordination among the various cryptologic organizations would result in much redundant and wasteful effort, and, more seriously for the German war effort, in missed opportunities. In the field of cryptanalysis, for example, three agencies– the Foreign Office, the Armed Forces High Command, and the *Forschungsamt* all claimed credit for the solution of a particular United States cryptographic system. Nevertheless, each organization continued to intercept and process independently all available traffic, apparently oblivious to the redundancy of these efforts, and to the need to compare and confirm results.

Another instance concerned the security of the main German cryptographic machine the Enigma.[2] Each branch of the German armed forces had its experts who expressed differing opinions concerning the degree of security this system afforded their communications throughout the war. They also differed on how long it could be expected to remain secure without modifications, and on techniques that could be employed by Allied cryptanalysts in attacking it, and thereby possibly compromising its traffic. But so far as is known, no coordinated effort was actually made to test this machine's traffic against their beliefs. Nor did they apparently recommend restricted usage of it on the basis of these beliefs.

The Enigma Machine

Additional redundancy, resulting from the lack of unified control, was apparent in intercepted German traffic. The same Allied nets were often copied by both Air Force and Army units, and their traffic simultaneously attacked by the two services. Even within the Army itself a lack of central control was evident.

[2] See the Fall 1974 issue of the *Cryptologic Spectrum* for discussions of this machine in the article entitled: "A Review: the Ultra Secret."

Moreover, dispersal of competent personnel among the various competing cryptologic organizations resulted in the loss of contact among specialists. Liaison in technical matters evolved into one based more upon personal relationships than on any specific technical needs. Also, the German Navy, with its traditional independence and aloofness, maintained an absolute minimum of contact with the other services in the area of cryptology.

Post-War Evaluations

Following the war, a number of leading German officers were questioned concerning their signals intelligence activities. They were asked, among other things, what they thought of other German cryptologic organizations, and to what extent a single over-all policy for all such organizations existed. Their opinions differed widely.

For example, General Keitel, Chief of the Armed Forces, and General Jodl, Chief of the Armed Forces Operations Staff, noted that they were aware of this duplication. Keitel further stated he attempted before the war to devise policy for its elimination, but that objections by Goering and Ribbentrop prevented its implementation. And after the war began, Keitel said that any further efforts at consolidation were dropped, and everyone "grabbed at everything."

Baron Joachim von Ribbentrop, Minister of Foreign Affairs, also recognized the fragmented nature of the cryptologic effort, and its inherent waste, noting that it "... was not well directed." He claimed to have held discussions to consolidate it, but "nothing happened." He further noted that he did not receive certain items which he had believed were available and which would have been of value to him.

Only Grand Admiral Doenitz, Commander-in-Chief of the German Navy, and Marshal Goering, indicated satisfaction with the situation as it evolved throughout the war. Doenitz's idea of signal intelligence was apparently limited to its naval applications, and he had not envisioned an over-all national policy, stating he would have made no change except to enlarge the Navy's involvement. Goering, on the other hand, had recognized in 1933 the need for cryptology on a "broad and general basis," giving this as the reason for founding the *Forschungsamt*, in which organization he expressed strong satisfaction.

All but Ribbentrop admitted the value of signals intelligence to their organizations, but there was no doubt that the only signals intelligence they trusted to any significant degree was that produced by their own organizations. Some were not even aware of the other organizations' roles, and if they were aware, avoided

Baron von Ribbentrop, Minister of Foreign Affairs, recognized the fragmented nature of the German cryptologic effort, noting that it "was not well directed," and that when he held discussions to consolidate it "nothing happened."

them to the maximum extent possible. Jodl, for example, noted that the *Forschungsamt* was "Goering's affair," and Keitel described the Foreign Office, about which he admittedly knew nothing, as "extremely secretive and jealous about everything their bureau produced." He also referred to the *Forschungsamt* as the "third competitor" and felt its reports were chosen on an "erratic and irrational basis."

Doenitz went even further, saying he had never heard of the Army unit, and had no information about the Air Force's organization, since these matters were of "no interest to him." Ribbentrop realized that the Foreign Office and Goering's *Forschungsamt* were covering the same field, but he claimed that the texts of the latter were less clear and often inaccurate. Hitler himself, according to Ribbentrop, expressed little interest in the German cryptologic effort, noting that Hitler "did not like this type of intelligence very much and . . . it was better to use . . . common sense."

Conclusions

From the foregoing discussions, it is seen that Germany, from 1918 to 1945, had no national cryptologic policy. Rather, six major organizations, and at least four of lesser significance, conducted its cryptologic business in an atmosphere of rivalry and suspicion. None had close association, much less coordinating authority, with or over any of the others.

This situation prevailed, to one degree or another, throughout most of World War II, severely hindering Germany's war effort, and resulting in redundant and wasteful effort and missed opportunities. Although German leaders recognized these shortcomings as far back as 1933, it was not until late in the war that a concerted effort was made to correct them. By that time, however, it was too late to effectively implement such a national policy, and Germany continued to suffer to the end of the war with a fragmented cryptologic effort.

[redacted] joined NSA in 1956; since then he has worked mainly in the collection and SRA fields, and at present with the NCS Press. He has contributed a number of articles to *Spectrum* and other Agency publications.

(b)(3)-P.L. 86-36