STANDARD FORM NO. 64

APPENDED DOCUMENTS CONTAIN CODEWORD MATERIAL

REF ID: A6 6628

Office Memorandum • UNITED STATES GOVERNMENT

TO : Mr. W.F. Friedman

DATE: 17 May 1954

FROM : L.D. Callimahos

SUBJECT: Draft of an historical brief on traffic analysis.

1. The attached history was prepared by Mr. R.S. Benjamin for inclusion as an appendix in the forthcoming NSA text on traffic analysis. The classification of the traffic analysis text will be Secret Codeword.

2. The original of this draft has been sent to CAPT Dyer for review and comments. This copy is for your information, and for any comments and suggestions that you may care to make.

L.D. Callimahos

~~SECRET AMBLE~~

Historical Background
of
Traffic Analysis
and
Communication Intelligence

(Draft of a proposed appendix to an NSA text on Traffic Analysis (~~Secret~~ Codeword) by Robert S. Benjamin, NSA-142K)

1 May 1954

Historical Background of Traffic Analysis and Communication Intelligence

1. Introduction

a. General. When did traffic analysis begin? Who was the first to perform traffic analysis and what were the circumstances? In searching for the answers to these questions, we soon realize that traffic analysis is in reality a very new subject because it is dependent primarily upon the existence of radio communication. The related field of cryptanalysis is hundreds of years old--writings dating back to the year 1474 are recorded.[1] But since radio was not invented until 1895, and not put to common use until after the invention of the vacuum tube in 1906, traffic analysis and radio communication intelligence are still less than 50 years old.

b. History of Electrical Communication

(1) A quick look at the history of the development of electrical communication will help to give us a backdrop against which we can study communication intelligence's beginnings and development. Morse invented the first practical electrical telegraph in 1835,[2] and Bell invented the telephone in 1876. The theory underlying radio communication was established by Maxwell and Hertz in 1865, but not until 1895 did Marconi send a message, over a distance of 1 3/4 miles. Several years later, in 1901, he received a message in

---

[1] Sico Simonetta's manuscript in Latin, written in Pavio, Italy, 4 July 1474. Ref. Articles on Cryptography and Cryptanalysis, op. cit., p. 187.

[2] As early in 1753, a letter to the Scots Magazine in Scotland suggested a "pith ball telegraph" which would consist of an insulated wire for each letter of the alphabet, ending in a light ball suspended over a piece of paper with the letter written upon it. As an electric charge came over the wire, the ball would attract the paper, and messages could thus be spelled out. Twenty years later such a system was built in Switzerland, and in other countries. Spark telegraphs, and telegraphs which indicated letters of the alphabet by electromagnetic deflection of needles were developed in the early 19th century.--- Encyclopedia Britannica, 1952 edition, Vol. 21, p. 882.

Newfoundland consisting of the letter "S" in Morse code sent across the Atlantic from England by assistants. De Forest in 1906 invented the vacuum tube, which made possible great and rapid advances in the development of radio. In 1909 the practical side of radio was dramatically brought before the public when 1500 lives were saved by the use of radio after the collision of the Republic and Florida.

(2) Radiotelephony developed in the decade from 1910 to 1920, and commercial radio broadcasting began in 1920 by the first station, KDKA, Pittsburgh. One of the first radio programs to reach the public was the news of the outcome of the Harding-Cox election returns in the same year. Teleprinters and "teletypewriters" started to come into general use about 1925, although forms of "printing telegraphs" are as old as Morse's invention, since his first model (printing dots and dashes) was a printing model. Television was conceived as early as 1920, and experimental broadcasting began in 1937. Frequency Modulation (FM) was invented as recently as 1939. Facsimile, which is not really a single device, but a whole category of devices, dates back to 1843, when Alexander Bain obtained a British patent covering the principle of electrical transmission of pictures. Other early workers, included Arthur Korn in Germany, Edouard Belin in France, and many others.

c. Military Use of Electrical Communication

(1) The first use of electrical communication in time of war was in the U.S. Civil War, when telegraph was used for calling up troops of the Union army, and used for the first time in a war in the field. War news had travelled so slowly before that time that in 1812, General Andrew Jackson won a victory over the British at New Orleans two weeks after peace had been

made.[3] Radio was not put to any practical military use in the field prior to World War I, although the British experimented with it in the Boer War in South Africa in 1899. The first field radio equipment in the United States Army appeared in 1903, and was used in maneuvers held in Kentucky. Since 1906, the principal armies of the world have had some radio equipment.[4]

(2) Radio was soon recognized as a valuable means of signal communication for forces whose movements were rapid. In World War I, the British entered the war with radio provided to a limited extent for independent cavalry. As the war progressed, the use of radio increased, and by the end of the war its value had been demonstrated not only to cavalry but also to aviation, artillery, tanks, and forward infantry units of the nations on both sides of the conflict.

(3) Between World War I and World War II, there was a period of further steady development of radio for military use. When World War II began, radio was universally regarded as a useful communication means in rapid-moving combat, and most armies were well-equipped with radio. There was for the first time extensive use of frequency modulation, particularly in front-line communication, and frequencies in the very high range. Teleprinter communication was used for high echelon military communication of the principal warring powers, except for Japan, which was backward in this regard. Radiotelephone was used extensively at low echelons and in mobile operations.

(4) In the following paragraphs, we will survey highlights of the history of communication intelligence from the standpoint of traffic analysis. Because they are an integral part of the same story, cryptanalytic developments will be discussed also, but in much less detail.

---

[3] Modern Communication, ~~op cit.~~, booklet published by Encyclopaedia Britannica, p. 21.

[4] Moran, Maj. R.B., in an article, "Powers and Limitations of Radio Communication within a Modern Field Army," Signal Corps Bulletin, No. 91, July-August 1936. Reprinted in Articles on Cryptography and Cryptanalysis, ~~RESTRICTED~~, published by Office of the Chief Signal Officer, 1942, p. 96

2. Analysis Prior to World War I (1906-1914)

a. The first record of radio intercept for intelligence purposes is in 1908, when the Austrians intercepted Italian radio traffic on the continent and at sea, and performed cryptanalysis upon it.[5] The Austrians were having a dispute with Italy concerning the annexation by Austria of Bosnia and Herzegovina. In 1911, the Austrians intercepted radio traffic from both sides in the dispute between Italy and Turkey--the first time that a neutral third party followed the military operations of two other nations at a distance, move by move.[6]

b. Also prior to World War I, the French maintained an organization called the Deuxieme Bureau of the French General Staff, which followed foreign radio traffic (especially German and Italian) for the purpose of developing knowledge which could be used in time of war.[7]

c. Although there is no record available to this writer of British activities in this field prior to World War I, it is known that active intercept of German Army and Navy traffic had begun well before the war. The Russians, Germans, and Italians apparently were still quite inept in the field of radio intercept or communication intelligence during this period.

d. The United States did not begin its radio intelligence work until during World War I.

3. Analysis During World War I (1914-1918)

a. General comment. It is of interest that the term "traffic analysis" does not appear in any of the available writings concerning communication intelligence activities prior to or during World War I, but the tech-

---

[5] Gylden, Yves, The Contribution of the Cryptographic Bureaus in the World War (World War I), ~~(RESTRICTED)~~, p. 21

[6] Flicke, Wilhelm F., War Secrets in the Ether, Parts I and II, ~~(RESTRICTED)~~, pp. 2, 3

[7] Ibid, p. 5

niques we now regard as comprising traffic analysis were used and spoken of as "W/T Intelligence," "radiogoniometry" (i.e., direction finding), "radio work," "evaluation," and simply "analysis." It was apparently not until World War II or the period preceding it that the term "traffic analysis" appeared.

b. The Allies

(1) According to available reference documents the British and the French apparently were the first to put to practical use the techniques of traffic analysis; both were using studies of this type in the early part of World War I. Concerning the British effort, Flicke tells us:[8]

> "The English were the first in World War I to create a technically exact and fast working system of evaluation, a system which can be regarded as modern today. 'Direction finding' stations were connected with each other and with the central office, and laid out here by the aid of silk threads on a great orientation map which was mounted horizontally. In the cipher bureau sat the men who day and night deciphered every incoming intercepted radiogram. An enormous card file containing all station callsigns which had hitherto appeared in the intercept service, along with all other available data, and this made it possible to recognize currently the systems according to which callsigns were changed in German traffic, to reconstruct these, and even to tell in advance what callsigns this or that German station would have tomorrow or day after tomorrow or a week hence. The collaboration between direction finding, evaluation, and decipherment was sensible and well-organized."

Gylden, a Swedish code and cipher expert, writing in 1931 along similar lines concerning analysis done in the British Navy, says:[9]

> "By a combined analysis of the location of the stations sending the radiograms, the callsignals (i.e., callsigns), the amount of traffic, and partial and complete cryptographic solutions, the cooperating radio and cryptanalytic services succeeding in very greatly facilitating each other's work and were able to bring the commander of the British Fleet extremely valuable strategic and tactical information."

---

[8] Flicke, War Secrets in the Ether, Parts I and II ~~(RESTRICTED)~~, p. 118

[9] Gylden, The Contribution of the Cryptographic Bureaus in the World War (World War I) ~~(RESTRICTED)~~, p. 20

(2) Early in the war, the French also were using techniques which we now associate with traffic analysis. They were able to distinguish the various German radio stations on the basis of the number of radio stations each contacted, and the duration of the activity of stations, and by the call-signs. Results obtained were studied against deciphered radiograms, and the activity of types of units and specific German units could thus be followed in detail.[10]

(3) The United States entered the war at a comparatively late date, in 1917, but for the period of our participation in the war, our Radio Intelligence Sub-Section made extensive use of traffic analysis principles, particularly in conjunction with direction finding. As enemy codes became more difficult to solve, increasing importance was attached to the Radio Goniometric (direction-finding) Service, Moorman tells us.[11] Another traffic analysis technique, study of message volumes, was used by the U.S. in studying German high command messages enciphered in a system called the "ADFGVX" system. By making a chart based upon the number of such messages intercepted, it was possible to discover certain things about the tactical situation, and, with some degree of assurance, predict what might happen.[12]

(4) There is very little information concerning communication intelligence activities of Russia, Italy, or other Allies in World War I, but they are believed to have been limited in scope.

c. Central Powers

(1) The Germans entered World War I ill-prepared for cryptographic and cryptanalytic work; there was a lack of understanding of both

---

[10] Ibid., p. 31. Also, Flicke, op. cit. p. 43.

[11] Moorman, Frank, Radio Intelligence Section, General Staff, General Headquarters, AEF, Final Report of the ~~(RESTRICTED)~~, p. 7

[12] Friedman, W.F., Communications Intelligence ~~(SECRET)~~, a lecture, 29 September 1950

fields, and in the Services there was a lack of personnel versed in these fields.[13] For the period 1914 to 1916, the Germans did practically no communications analysis of any sort, although they were early alerted to the values of communication intelligence during the Battle of Tannenburg in August 1914, when the Russians used radio extensively for the transmission of many messages in the clear, and the German High Command made many of its crucial decisions based on the knowledge thus gained.[14] The Germans came to be more efficient in this field toward the end of the war, although there is no evidence that they performed integrated analysis studies of the type carried on by the British and the French.

(2) The Austrians, as we have noted, already had a cryptanalytic service before the war, and were thus able to gain almost immediate successes in this field against the Russians. A succession of cryptographic and communication blunders on the part of Russians made it possible for the Austrians to know intimate details of the Russian's troop dispositions and intentions. Against the Italians, the Austrians used some of the methods of traffic analysis. Gylden writes:

> "During the frequent changes of call signals made in the Italian Army, the great majority of the radio stations tried, for purposes of control and check-up, to get in contact with the other radio stations, both those located near them and those located far away. This gave rise to the circumstance that many stations which had been silent for some time betrayed their location. They were identified by radiogoniometry. We can readily understand the importance for the Austrian Command of being able in this way to check up periodically, at least in the main, on any changes that might have been made in the grouping of the Italians."

---

[13] Gylden, op. cit., p. 17, 43

[14] Wlicke, op. cit., p. 27 ff.

Later in World War I, Italian cryptographic system[5] underwent vast improvement (probably as a result of assistance from the French), and subsequent results of the Austrian intercept service were as a result of techniques other than cryptanalysis--probably including direction finding, traffic analysis, and espionage.[15]

4. Analysis Between the Wars (1919-1939)

a. General Comments. Developments in the field of communication intelligence between World War I and World War II were slow--there was naturally a great decline in efforts in this direction. The writer has been able to find no record of radio intercept in connection with the only large military actions in the period, the Italian-Ethiopian war in 1935 and the Spanish Civil War in 1936. In general, organizations performing analysis or cryptographic development were cut to minimum size and operated under difficulties. It was, however, a period of development; in Europe, nations followed each other's military maneuvers and minor skirmishes, and in America there were developments in the field of cryptography.

b. United States. The Cipher Bureau (MI-8) in the Military Intelligence Division of the War Department, which had been created on 10 June 1917, moved in August 1919 to New York City where it continued to function until November 1929 as a highly secret and well-hidden signal intelligence agency of the War Department. This group was the "American Black Chamber," concerning which H.O. Yardley, its head, wrote a book after it was discontinued in 1929 when the U.S. State Department withdrew its share of funds supporting the organization.[16] There was continuous effort in the

---

[15] Gylden, p. 80, 81.

[16] The publishing in 1931 of Yardley's book, which discussed techniques of cryptanalysis of codes which were still in use, has been generally blamed for making the tasks of all communication intelligence much more difficult than formerly. Its revelation of the solution of Japanese diplomatic messages relating to the Washington Disarmament Conference of 1929 is believed by many observers to have led to the Japanese denunciation of the naval limitation treaties in 1935.

communication intelligence field by the U.S., however, because a separate group in the Military Intelligence Division which had been in the code compilation business from 1921 to 1929 was transferred to the Office of the Chief Signal Officer in 1929, and was given both code compilation and solution responsibility.

For the period 1929 to 1939, this small group, suffering from lack of adequate funds, operated as the Signal Intelligence Service and laid a groundwork for later expansion. Plans for this expansion were accelerated in the period following the mounting tension in Europe; intensive training of selected people in cryptography and cryptanalysis was undertaken by extension courses, and steps were taken to improve United States cryptographic systems.

c. France, Great Britain, and Other Countries. According to Flicke, during this period the French had an active intercept service whose focal point was directed toward the observation of foreign armies. The British maintained a comprehensive effort aimed at complete coverage in the international political field. The Italians, although well equipped from a technical standpoint, fell far behind the British, Germans, and French, in the field of results. Flicke also asserts that many other countries, including Czechoslovakia, Poland, Russia, Austria, Hungary, Finland, Lithuania, Spain, Yugoslovia, Norway, Denmark, Portugal, and Sweden also maintained communication intelligence efforts on a larger or smaller degree. The cooperation between various combinations of these countries in the intelligence field was a tangled web of intrigue and counter-intrigue.[17]

d. Germany. After World War I, there was a cutting back of communication analysis effort in Germany, but at least a sub rosa continuation

[17] Flicke, op. cit., p. 202 ff

of it, Flicke tells us.[18] There were two organizations at the time, one in the Foreign Office carrying out cryptanalysis of foreign diplomatic cryptographic systems, and the other, in the Ministry of Defense, crypt-analyzing and evaluating results of foreign military radio traffic. The emphasis in the latter group was on the "evaluating," which included systematically piecing together numerous single phenomena in foreign radio traffic for the purpose of getting an over-all picture of the situation in the area being observed.

Beginning in 1928, there were a number of military maneuvers which gave the German analysts good experience. In that year, the British held Rhineland maneuvers; in 1929 there were maneuvers in Czechoslovakia; in 1930 and subsequent years there were a series of French military and air maneuvers which were observed by the Germans.[19]

e. Japan. Very little is known concerning the efforts of the Japanese in the field of communication intelligence prior to World War II. They apparently performed little original analytical work, judging by the writings of Toshiyuki Yokoi, a Japanese Naval cryptanalyst.[20] They solved a U.S. Navy strip cipher in 1932, and succeeded in surreptitiously photographing an American diplomatic code in 1933. A Japanese naval officer and an assistant came to the United States in late 1937 and travelled all over the East and West coasts, secretly intercepting U.S. Naval broadcasts and piecing together information concerning our Navy's performance, morale, and training routines. By 1938, the Japanese had intercept stations through-

[18] Flicke, op. cit., p. 166

[19] Flicke, ibid., p. 191

[20] Yokoi, Toshiyuki, The Japanese Version of the Black Chamber, published by NSA-18 as HF-304.

out their entire Pacific Ocean area, and after studying annual U.S. Naval maneuvers, Yokoi reports that "it was possible to obtain fairly accurate estimates of enemy conditions by the use of the wireless direction-finding apparatus and by learning the enemy's communication condition even though the enemy codes could not be read. It was learned that this was very advantageous when making an estimate of battle plans."

5. Analysis During World War II (1939-1945)

a. General Comments. During World War II there were a number of dramatic incidents which had behind them accomplishments by the cryptanalytic bureaus of the warring nations--Yamamoto was shot down; the Battle of Coral Sea was brought to a successful conclusion largely as a result of successful United States cryptanalysis of a Japanese Naval Code; throughout the war the Allies were successfully exploiting German cryptographic systems. On the other hand, the Germans were successfully reading many Allied systems, which, for example, accounted for Rommel's initial successes in North African battles. Behind all these successes, however, traffic analysis was playing its part in a very valuable way by providing a steady flow of intelligence information throughout the war when successful cryptanalysis was not possible, and by providing a framework within which decrypted messages could be interpreted when cryptanalysis was successful. The importance of communication intelligence in World War II is probably best summarized by the following statement which appears in the Report of the Pearl Harbor Investigating Committee of the 79th U.S. Congress:

> "All witnesses familiar with communication intelligence material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

b. United States.

(1) During the early part of the World War II, the communication intelligence organization of the United States War Department underwent a series of changes in designation, but for the last two years of the war, it was called the Signal Security Agency. On 15 September 1945, it became the Army Security Agency, and was detached from the Signal Corps, and established as a separate organization under the assistant of Chief of Staff, G-2. During the War, the United States Navy maintained a separate communication intelligence organization, called OP-20-G, which cooperated with the Army organization. The Army Security Agency had the assignment of producing communication intelligence of both enemy ground forces and enemy air forces; OP-20-G had the mission of producing communication intelligence of enemy Naval forces.

(2) The United States and Great Britain cooperated in the communications intelligence field throughout the war. As a result of agreements made during 1942, the United States accepted primary responsibility for producing intelligence concerning the Japanese in the Pacific Theater and Great Britain had as its primary responsibility to produce intelligence concerning the Germans and others in the European Theater. This division of effort applied to all the military services, and to both cryptanalytic and traffic analytic effort. Intercept coverage was split roughly along the same lines, but both ourselves and the British provided supporting cover and limited analysis in the other's sphere of responsibility.

(3) A great deal of success was achieved against the Japanese in all phases of the communication intelligence effort; Japanese army, air force, and naval codes yielded to cryptanalysis, and traffic analysis provided

a continuing picture of the Japanese radio nets. Field processing centers located in Australia and India worked on the Japanese army and air force problem, but the main effort was in Washington. The main effort on the Japanese naval problem was in a field center in Hawaii. Other supporting naval field centers were located in Australia and Ceylon, and specialized technical research was carried on in Washington.

(4) In the first year of the war, the United States studied German communications, but after BRUSA (British-United States) agreements in the field were reached, the primary effort was carried on in England.

c. Great Britain and British Commonwealth

(1) The British communication intelligence organization was called Government Code and Cipher School (G.C.&C.S.) during World War II. As intimated in the previous paragraphs, the British analyzed the German's communications, and also those of the Italians, achieving great success both from a traffic analytic and a cryptanalytic standpoint. The fact that the British had continued intercept efforts in the period between the two wars enabled them to change quickly to a wartime footing with a minimum of wasted effort. In addition to work on the two major enemy targets, the British intercepted and analyzed the radio traffic of many other European nations.

(2) Australia and Canada had fairly large communication intelligence organizations during World War II, both of which were directed primarily at the Japanese problem in the Far East, and which worked very closely with the United States.

d. Russia

(1) Little information is available concerning the operations of the communication intelligence organization of the Soviet Union during

World War II, but it is certain that its efficiency had vastly improved since World War I. Flicke, speaking from the viewpoint of the defeated Germans, ventured the opinion that the Russians lost the radio intelligence phase of World War I, but that they won it in World War II.[21] They had taken tremendous strides in the field of communication security since their World War I errors, and on the basis of available documents, it can be assumed that by the time of World War II they not only possessed knowledge of advanced cryptanalytic techniques, but also were well aware of and used traffic analysis potentialities.[22]

(2) Flicke reports that from the spring of 1942 on, the Russians were extremely well informed about the German combat strength, intentions, and all phases of their battle order. Although much of the information probably came from partisans, some from prisoners of war, and some from agents, there was no question in his mind but that the Russians must have succeeded in reading German ciphers.

(3) A partial picture of the Russian intercept service in the early part of World War II is given by an interrogation of the former operations officer of the Soviet fixed intercept station,[23] in Minsk a Sergei Grigorivish, who was captured by the Germans in early 1942. At that time, the Russian Army had a series of fixed stations in the Far East and West, as well as a number of intercept battalions attached to Military Districts in the Western USSR. Presumably the Navy and Police also had their separate intercept services and intercept stations. Assignments were passed on to the intercept operators together with such information as was necessary to cover targets efficiently.

---

[21] Flicke, War Secrets in the Ether, Part III, p. 492 (rough draft)

[22] Particularly valuable in this respect is a Soviet-prepared Manual For the Analysis and Utilization of Radio Intelligence Material, (Moscow, 1944), which in four chapters outlines the Soviet approach to traffic analysis. (TOP SECRET)

[23] A fixed station is one in permanent quarters, not designed for a mobile operation.

According to the interrogee, no analysis was carried on at the station. Compartmentation of personnel was carried to extremes--the operation of the intercept units was apparently fairly efficient, although the people at the station had no knowledge regarding the degree of success on various problems. At Moscow, communication intelligence was carried out in the Intelligence Section of the Peoples' Commissariat of National Defense (NKO), which consisted of a number of separate evaluation sections.[24]

e. Other Allies. Although it is almost certain that many of the other Allies such as France and Norway were also in the communication intelligence game, there is no information available to this writer concerning their operations.

f. Germany

(1) During World War II, the Germans placed great reliance upon radio intelligence as a prime source of operational intelligence. Contrary to Allied practice, the Germans appear to have concentrated on low level radio nets for their cryptanalytic and traffic analysis studies. As a result, their tactical intelligence effort benefited, but their strategic intelligence effort suffered.[25] The Germans claim to have been particularly successful in their traffic analysis of American, British, and Italian communications, but as the war progressed, they had increasing difficulties against the Soviets in getting a clear picture of the radio situation.[26] Allied air communications proved especially vulnerable.

(2) The importance which the Germans attached to traffic analysis can be appreciated by considering statements made by several German prisoners of war:[27]

[24] The Russian Y Service ~~(TOP SECRET)~~, NF-82, published by CSGAS-14, 29 Sept 47.

[25] German Operational Intelligence, ~~(RESTRICTED)~~, p. 27

[26] Flicke, op. cit., p. 359,443;also EXCERPTS FROM GERMAN TICOM REPORTS ON TRAFFIC ANALYSIS, ~~(TOP SECRET)~~, p. 1

[27] EXCERPTS FROM GERMAN TICOM DOCUMENTS CONCERNING JAPANESE AND GERMAN T/A",p.4

JODL: "Another important success, as far as analysis of military traffic was concerned, was working out the Allied order of battle. This information was particularly important for a knowledge of the situation in England prior to D-Day, and was obtained mainly from traffic analysis."

LUDWIG: an expert on Allied Air Order of Battle: "It can be stated that no attack of the 8th Air Force came as a surprise. General advanced warnings were given some hours before the raids."

TRANOW: "All squadrons and groups in these commands (the IX, XIX, and XXIX Tactical Air Commands) had fixed callsigns. These callsigns were known without exception from our observation and from captured material. From this, we could say on every raid what unit and the type or types of planes in the formations were on the way."

(3) In the writings of German authorities on communication intelligence, the statement is made that normally German intelligence from this source accurately appraised the situation, but that particularly toward the end of the war, Hitler consistently refused to heed its warning, but preferred to trust to his own intuitive hunches as to what the true situation was.[28]

(4) As an indication of the scope of German communication intelligence, it is reported that in 1945 at the end of the war there were 12,000 persons engaged in the effort in the German Army alone.[29]

g. Italy. Information concerning the Italian intercept and analysis effort is lacking. By inference, however, we can surmise that the Italians were not overly-skilled in the art of communication intelligence, since they made a very poor showing in their campaign against the Greeks in 1941, using the same communications data they had used in the previous year in their maneuvers, and their radio nets could be easily followed, yielding much intelligence.[30]

---

[28] Praun, German Radio Intelligence, ~~CONFIDENTIAL~~; p. 112;

[29] ibid. p. 161

[30] Flicke, op. cit., p. 359 (unpublished rough draft).

b. Japan

(1) According to Flicke, just prior to their joining forces with Germany against the Allies, the Japanese Ambassador to Germany, Oshima, sought and received complete cooperation with the Germans in the field of cryptanalysis (presumably including all phases of radio intelligence), as one of the conditions for entering the war on the side of Germany and Italy against the United States, Great Britain, and the Netherlands.[31]

(2) The performance of the Japanese in the field of communication intelligence was only fair; they had much difficulty in their attempts to read our cryptographic systems. Interrogation of several Japanese Naval Intelligence officers revealed details concerning the communication intelligence effort, particularly traffic analysis.[32] The center of activity was at Owada, Japan, where Allied transmissions were intercepted, copied, and analyzed by areas. Traffic analysis was used in conjunction with direction finding to produce intelligence; particular attention was paid to peaks in traffic volume as representing a "crisis," although the Japanese could not necessarily tell where the crisis would materialize.

(3) From a TICOM report based on other interrogation of Japanese prisoners of war, we read:

> "The Japanese Army had great difficulty in obtaining operational intelligence due to its failure to break enemy codes and to lack of systematic research....In order to cope with this situation, the Army as a counter-measure resorted to the evaluation of intelligence by means of traffic analysis beginning 1 October 1944."[33]

---

[31] Flicke, op. cit. p. 458 ff

[32] Interrogation No. 431 (~~RESTRICTED~~) and No. 808 of the Japanese Intelligence Section, G-2, USSBS, dated 20 November 1945. Cited in "Enemy Traffic Analysis," article in July 1946 issure of Security Bulletin, published by U.S. Chief of Naval Operations.

[33] "Excerpts from Ticom Documents concerning Japanese and German Traffic Analysis", (~~SECRET~~), p. 10

Apparently the Japanese considered cryptanalysis and traffic analysis to be an "either-or" proposition, and did not appreciate the fact that for best results the two work together as a team.

6. Analysis Since World War II (1945-1953)

a. General Comments. The period since the close of World War II has been marked by a continuation of almost full-scale communication intelligence efforts by principal nations of the world, in contrast to the period between World War I and World War II when activities in this field were greatly diminished. The continual world tension, and the United Nations police action in Korea beginning in 1950 were motivating factors.

b. United States. Several reorganizations have been the most significant developments in communication intelligence in the United States. Whereas there had been separate organizations for the Army and the Navy (Army Security Agency and OP-20-G, respectively), the Air Force officially entered the communication intelligence and security field with the formation of the Air Force Security Service in ____. Amost simultaneously, in May 1949, the Secretary of Defense (in the trend toward unification of the services) authorized the formation of the Armed Forces Security Agency (AFSA). The basic directive states that the Armed Forces Security Agency was established in order to provide for the placing under one authority the conduct of communication intelligence and communication security activities within the National Military Establishment, except those which are to be conducted individually by the Departments of the Army, Navy, and Air Force. Later in October 1952, AFSA became the National Security Agency (NSA), which had broad powers over all phases of communication intelligence activities carried on by the U.S. The three separate service organizations continued to exist, with their activities being generally integrated and delineated by NSA.

At the close of World War II, the United States gradually re-orientated its efforts in the COMINT field toward Soviet Russia and the Communist block of nations. The major field of study has been the Russian problem, with efforts also being directed at Communist China, the Greek Guerillas, North Korea, Yugoslavia, and certain other nations.

The United Nations police action in Korea from 1950 to 1953 was a fertile field for communication intelligence. The U.S. was quite successful against the Communist China and North Korean opponents, particularly in low level radiotelephone intercept from forward positions. In the air phase of the action, radio intelligence also played an important role. Many commanders who had previously been skeptical of the value of COMINT became convinced of its value through experience, and at the same time realized more clearly the importance of communication security.

c. Great Britain and the British Commonwealth. The British and Canadians, particularly, continued to cooperate with the United States in the communication intelligence field. In the interests of economy and

[redacted]

[redacted] Other developments during this period in the British organization, now called Government Communication Headquarters (GCHQ), and in the Canadian organization, Communications Branch, National Research Council (CBNRC), have paralleled United States developments.

d. Russia. Our knowledge of developments in the communication intelligence field in the Soviet Union since World War II is very sketchy. From isolated scraps of information, however, it can be stated that an extremely efficient organization continued to be active in the field of

radio intercept, and that fairly finished analysis was being carried on at field centers for the benefit of important local commanders, with copies of these reports being transmitted or couriered to higher intelligence headquarters. The Soviets continued to make active use of radio direction finding in locating radio transmitters of others.

Again details are not known, but it is suspected as likely that close cooperation has existed between intercept services of Satellite nations and the services of Russia.

e. Other countries. It is known that active intercept and analysis organizations functioned after the war in a number of other European countries, including France, Italy, West Germany, Sweden, and Norway.

f. Concluding remarks. The history of communication intelligence continues to be written, and as future events unfold, it will continue to play the important role of furnishing hard-to-get intelligence which can assist our nation's leaders in the formulation of policies and in future military actions. Although communication intelligence has perhaps had its most dramatic moments in times of war, it can and has contributed much to the prevention of war, and should not be thought of primarily as a war-time activity.