REF ID:A71138

CONCERNING CAPTURE OF M-209 KEY LISTS BY GERMANS

1. ([redacted] IF-107)

"In June 1943 an M-209 key list for the month of June was captured in Sicily. The capture was not apparently reported because traffic was sent and read on the captured keys during the entire month of June.)

2. ([redacted] of OKH) (I-23)

"In the Nettuno bridgehead a Battalion Commander of the 45th U S Infantry Division was captured with all the Division's keys on him and all the call-signs for the month with left and right neighbors and with the rear."

3. ([redacted] of OKM/4 SKL III)(I-95)

PL 86-36/50 USC 3605

"A month's traffic over one of these machines was read at the end of the African campaign because the army had captured the cipher sheets for that period."

4. ([redacted] of OKM) (I-93)

"The only pinch we got concerned the Hagelin machine in the Sicily area. This pinch was towards the end of July or beginnin of August 1943. The captured material was out of date only a few days later. We also captured some American cipher instructi for use with the Hagelin machine. The instructions and keys were valid for one month: for July. In consequence they were in force for a few days after the pinch was made."

5. ([redacted] of OKH) (I-142)

"PW thinks that the Germans had captured cipher instructio in Sicily which had been lost by an American armored unit."

4. [redacted] stated that from interception of Air Force traffic they were able to get up to the minute weather reports from monitoring the radio-telephone conversations, and from traffic of the Sea Rescue aircraft which passed Syko and also clear text messages. (I-109)

5. [redacted] an evaluator with OKH, claimed that in 1942 the Germans had been able toreconstruct a very complete picture of the United States Army organization from their intercept of plain-text transmissions within the United States. File indexes of Army officers down to Captain, names of units, and the location of these units were compiled. This information was given to the General Staff who issued pocket manuals of the United States Army. According to [redacted] it was claimed that 95% of the information contained in these volumes came from radio intercept. ((NB. I do not like [redacted] statement because I have not been able to check his veracity. This in spite of the fact there are other references which do mention German intercept of radio traffic within the United States, and of several references where mention is made of the existence of such a manual. It is quite possible that [redacted] is correct, but my impression is that most of

his information came from hear-say. It is true that he worked as an evaluator on the consolidation of reports from various Signal Intelligence units and may have been in a position to have accurate knowledge. On the other hand he was only a Sgt. in the German Army and I do not believe the average German soldi was in a position to have access to such knowledge.))) (I-76)

Slidex: [redacted] mentioned our Slidex and remarked that the traffic was broken with ease every day, mainly because of the stereotyped messages, usually dealing with the weather. The idea was to go out and have a look at the weather and then return to deal with the messages. (I-74)

PL 86-36/50 USC 3605

[redacted] (of OKH) stated that the 117th Recon Troop of the VI Corps used a system similar to Slidex, having a much larger card and using complete alphabets on both the vertical and horizontal strips, which changed only every 30 days. This system differed from Slidex in that "no clear text was used". (I-76)

Combined Assault Code: "For inter-Allied traffic in landing operations the Combined Assault Code was produced by the Combined Communications Board, Washington. There are presumably two identical series of this 3-letter code, which is used only unenciphered. One of them is used in the Mediterranean and the second on the Channel coast. The 4-letter pronounceable indicator of the latter begins with "A", of the former with "B". The following indicators appeared: ADCO, first appeared 28/4/44 in training traffic. AGOG first appeared 6/6/44. After we

had already made good progress in interpreting it we captured it and it was thereupon prematurely withdrawn. ALBA appeared 21/6/44. AMID appeared 24/8/44, and AQUA appeared 28/10/44. We succeeded in decoding ALBA, AMID, and AQUA quite extensively. The messages contained reports of supply convoys and organizational measures in the invasion areas. Recently they were largely weather reports. The volumn of traffic, which at the start of the invasion, was over 100 messages a day, has in the meantime sunk to two to four messages a day." (D-15)

((According to our records in Security, the CAC was a 3-letter, two part, unenciphered code intended to provide security only in the initial stages of amphibious operations. It was first used in the North African invasion. Different code books were used for each new invasion. Our security studies indicate some 400 messages and a crib needed for partial reconstruction.)))

Bomber Code: Used by U S 8th Bomber Command and IX Bomber Command.

Daily change was made at 1800 hours. "It often happened that captured codes from aircraft shot down at night were recovered so promptly that they were available next morning at the start of the 8th Air Force's operation." (I-109)

Rekoh: [redacted] of OKL). "In order to become familiar with the contents of Rekoh card messages, which were used by the Americans on the Atlantic Ferry routes, one day's traffic, which was especially favorable, and consisted of about 60 messages, was deciphered in mid-March of 1944 by the 16th Company of LNR 3 in Angers. The evaluation section was not especially interested in

the contents of these messages and therefore work on them was stopped."

Aircraft Movement Code: ([redacted] of OKL)

"As with its British counterpart, this system was introduced at a relative late date and was found by the German SIS to be identical with the British system. It was used for ferry flights over the Atlantic and West coast of Africa. Even when the system could no longer be deciphered because of frequent changes, the approximate number of aircraft being ferried could still be determined by the evaluation section from the depth and numbers of groups of the messages, as well as by the time of day at which they were sent."

PL 86-36/50 USC 3605

Capture of Keys: (by [redacted])

"G suggested that the U S procedure for reporting capture of keys be tightened up. He seemed to feel that we were more lax in this regard than the Germans, and that this was a very grave menace to our cryptographic security."

Double Transposition: ([redacted] of OKH) (I-80)

"A key for this system was captured in France after the landings on D-day, but, as it had been compromised, the system was not used on the Western front. It was used in Italy in February of 1945."