LECTURE VI

We begin now the final session in my series of talks. It will be devoted to four main topics:

1. First, what sort of codes and ciphers were we confronted with immediately before and during WWII?

2. Second, what were we able to do with them and how did we do it?

3. Third, what sort of protective measures were taken to enable our high-level authorities and commanders to use the results of the COMINT efforts and activities?

4. Finally, what are the prognostications for the future?

Let's begin with the first of the four topics. What C's and C's, or technically speaking what cryptosystems were we confronted with immediately before and during our participation as a belligerent in WWII?

A. In the European theater, there was, of course, the problem of tackling a multiplicity of pretty high-grade cryptosystems of the Germans.

1. Take first: the diplomatic ones, of which there were two very high-grade systems. (1) Floradora, (2) GEE (3) Agents (All this and heaven too) and miscellaneous.

2. The cryptosystems of the German Wehrmacht or Armed Forces:

(1) Low-level codes, (2) Double-PLAYFAIR, (3) Raster, (4) E a- 3 wheel b- 4 wheel and Uncle Dick, (5) Fish a- Tunny b- Later fishes .

B. The Italians. But these we were concerned largely only with the Diplomatic area. By the time our forces were in direct contact with Italian military, they were pretty well disorganized and what communications there were, were in G systems.

C. In the Pacific Theater.

1. The Diplomatic systems.

a. Codes, and codes enciphered with transposition.

b. Red

c. Purple

2. Military.

a. Attache, b. Ground forces, C. Green, d. E. machines.

3. Naval.

JN-25, Naval attache.

As long as we are dealing with cryptosystems might as well show and tell a bit about the Russians.

65
66
196
196.1
Difficulty of identifying traffic. M-211. Coleridge. Longfellow. Double-tape (Pagoda). Albatross. Scrambler. OTP.

Principal operations of COMINT: (1) Intercept (incl. D/F, RFP, TINA), (2) T/A (remarks on validity, (3) Cryptanalysis, (4) Translation and emendation, (5) Large scale production or exploitation, (6) Evaluation of information (military intelligence), (7) Collation with other sources, (8) Dissemination.

Let's dispose of T/A first. T/A is very important for two reasons: (1) Establishing networks when callsigns and frequencies change frequently, as in the case of the German Armed Forces, (2) In absence of decrypts, is highly useful and may be the only source of COMINT.

255
256
254

RFP and Morse Op. Identification.

238
239

Information from ebb and flow of traffic.

Read from "All honorable men".

238.1

Graph illustrating derivation of important intelligence by traffic analysis in World War II - convoys across the Atlantic from HAMPTON Roads to Algiers. This chart shows a daily breakdown by security classification of the traffic from Hampton Roads Port of Embarkation to Algiers, North Africa, for the month of April, 1944. Three definite peaks in traffic volume are evident, each of which indicates a convoy movement from Hampton Roads to Algiers.

238.2
The approximate size of a movement is judged from the totals of messages and groups in the peak period, while the destination and route are given away by addressee call signs in the messages. Close inspection will show the first traffic surge began on 4 April, the second on 13 April, and the last on 22 April. Experience has shown that these traffic peaks appear on the circuit a day or two following the actual convoy sailing date. The convoy movements are therefore "called" on the 2nd, 11th and 20th of April. Furthermore, the traffic study shows definitely the
238.3
proportions of supplies and troops carried in each convoy. This is due to the fact that all passenger messages are classified SECRET; cargo messages are CONFIDENTIAL. Detailed analysis shows that there were 21,836 CONFIDENTIAL groups, and 3,965 SECRET groups transmitted in connection with the 2 April convoy. The next convoy gave rise to 18,160 CONFIDENTIAL and 4,470 SECRET groups. The third convoy required 19,429 CONFIDENTIAL groups and 594 SECRET groups. It is apparent from these figures that the major function of each of these convoys was to carry equipment and supplies.

254
255
256
RFP I & II - Two different transmitters. TINA or Morse Operator Identification.

Cryptanalysis -- most important steps.

(1) Study external characteristics of messages, (2) Study any available collateral including that obtained from previous solution "crypt-continuity", (3) Study beginnings and ends of messages, (4) Search for repetitions between and within messages, (5) Preparation of statistical counts of letters, groups, etc., (6) Search for indicators, (7) Determine type of cryptosystem used, (8) Separate traffic into groups of messages in same or related keys, (9) Test for probable words, stereotypes, analogies, isologs, homologs, (10) Reduce to simplest terms.

The rest of my talk will be devoted to a brief discussion of modern, practical cryptanalytic operations and gadgetry.

245
Trithemius. (his photo matches the mental picture the average layman has of a cryptanalyst)

The veil of secrecy has produced an air of mystery. Before the World War II, it was possible to do much processing merely with pencil and paper. Now crypt-analytic work is a very big business--complex, expensive, but pays big dividends.

Tell Semiramis story.

131
Cryptanalysis of modern systems has been facilitated by the invention, development, and application of special cryptanalytic aids by way of machines. The nature of the problem--not merely the number of permutations and combinations but

the type is more important--question of testing out multiplicity of assumptions and hypotheses, commonly by statistical methods. High-speed testing is secret!

Earliest cryptanalytic devices at Riverbank Laboratories.

134
My memo begging for one set of IBM, dated 30 October 1934.

Navy began using IBM in 1932. Combined total 1934 - 8, 1945 - 750. Now in NSA (1954) - 314.

135
Extract from first contract with IBM. Tell how got it put over--QMG's office had IBM installation for CCC accounting. Cancelled when an old-timer can't see any new-fangled notions.

141
One wing of IBM installation in WW II.

The basic and most important analytic machines we had were those for German Enigma. The Navy Bombes - 90 sets of 4 high speed computers each running at 18,000 r.p.m. The Army Madame X - Electrical relays. Regret I have no slides to show of those. Explain why.

147
Geheimschreiber.

150
150.1
The Japanese "Purple" - our version.

Both Army and Navy had additional specialized machines but I can show slides only of the Army types. Don't know whether Navy took any pictures but they had as many and as complicated machines as Army.

Duenna - tell of general solution not dependent on cribs.

To find coincidence count in pair of messages, 200 letters each at all possible juxtapositions will require 40,000 comparisons. By hand 10 hours @ 1/second. ROBIN does it at 50,000 per second.

70 mm comparator was first machine. Built in late 30's by British MIT, put in to service 1942. 85 letters/second. COPPERHEAD - to search for two group bits in enciphered code. Put into use in 1944--now obsolete with 701 computer.

253 - Alcatraz - monographic and digraphic frequency counts.

145 - Machine decipherment.

137 - Locating repetitions - "Brute force" machine.

138 - Locating repetitions - "slide run".

139 - Another machine for decoding and deciphering.

140 - CAMEL.

145 - CAMEL Code indicator locator.

144 - Assembly of components.

200.1 - JAS deciphering.

201.1 - Selective J-square.

202
202.1 - J-square permutor

142 - Purple dudbuster.

199
199.2 - GEE additive generator (typing)

198.1 - Geheimschreiber crib-tester.

143.1 - Auto-scritcher (Rodin)

248 - O'Malley - Specialized arithmetic computation. Gives summations of products of pairs of numbers.

249 - DEMON II.

250 - Goldberg - Coincidence machine, general purpose, large scale. First NSA one
251 with magnetic drum for storage.

259 - ATLAS.

New machines: CONNIE I - Teletype scrambler - 5000/second and print.

II - teletype scrambler greater flexibility.

VIVIAN - Comparator using mercury delay line.

DELLA - 5 million comparisons/sec as against ROBIN's 5000.

137 - A "brute force" machine.

138 - A machine for matching messages.

143 - The "Auto-scritcher" - Rodin - The Thinker.

145 - An analog. This was for JAS system - Jap MilAtt.

248 - O'Malley. Specialized arithmetic computation. Gives summations of products of pairs of numbers having up to four digits.

259A - ATLAS.

Assistance we had from British.

A. I had hoped to show slides or charts of Battle of Atlantic - explain.

B. Principal reasons for success:

1. European theater.

a. German lack of imagination.

b. Failure to change rotors.

c. Stereotypy and methodicalness of German mind so that cribs and cross-cribbing possible. Passing messages from one net to another without paraphrasing.

2. Pacific Theater.

a. Lack of technical know-how.

b. Complexities piled on complexities and dependence thereon for security.

c. Errors therefore.

d. Methodicalness and stereotypy.

3. Brilliance of UK-US crypt.

What we owe to UK crypt.

4. Money to spend on COMINT activities.

Read from Brownell Report.

234
Chart showing processing steps from originator to consumer (Army).

235
Chart showing no of "bulletins"

Navy C.I. organization. Combined C. I. organization.

Extracts from Part II, Brownell Committee Report. (June 1952)

In World War II COMINT may well have been our best paying investment. Its costs cannot be accurately computed but an informed guess would be perhaps 1/2 billion dollars annually.

General Handy is reported to have said it shortened the war in Europe by at least a year.

In the Pacific, COMINT located the Japanese fleet enroute to the Coral Sea and again enroute to Midway in 1942, enabling us to mass the carriers for the battles which generally is regarded as the turning point of the war against Japan.