SCAMP 1958

LECTURE VI - 3 July 1958

Section 1 -

WW II Systems

126 - Double Playfair

131 - Raster

1361 - "

1362 - "

Lecture VI – 3 July

238-1
238 2
238.3
254
255
256
245
131
134
135
141
253
145
137
138
140
145
144
200.1
201.1
202
202.1
142
199
199 2

148.1
143.1
248
249
250
251
259
234

147
150
150 1

} go in here 8

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 + 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 + activities?
4) Finally, what are the prognostications for the future?

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

170.1 — 170.9

171 – M-461 – Ft Monmouth

175 – Fuel data

176 – holes

61 – 64 IMT

177 – CCM

178 – 1861 — ?? How many to show

H4 + Hagelin 1931

261 + A + B

230 Orville Wright

129, 130 changing of material

Let's begin with the first of the four topics. What part of codes and ciphers, or technically speaking cryptosystems were we confronted with immediately before and during WW II?

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

1. cryptosystems of the Germans. Take, first, the diplomatic ones, of which there were two very high-grade systems
   1) Floradora
   2) GEE
   3) Agento (ACA this + heaven too) ← Miscellaneous

2. The cryptosystems of the German Wehrmacht or Armed Forces:
   1) Low-level codes (3) Fraster
   2) Double-Playfair
   4) Enigma a) 3 wheel + Uncle Dick
      b) 4 "
   5) Fish a) Tunny
      b) Lateral fishes || Depth

A The Italians ~~will disappear from~~
But these we were concerned with largely only in the Dip area
By the time our forces were in direct contact with Italian military, they were pretty well disorganized & what com there were, were in G systems

C In the Pacific Theatre
1 The ~~Dip~~ systems
a Codes, enciphered with transp
b Red
c Purple
~~d Typex~~
2 Military
a Attaché
b ground forces
c Green
d Marines

3 Naval
JN-25
Naval attaché

[R - systems next card]

As long as we are dealing with cryptosystems might as well show + tell a bit about R

Difficulty of identifying traffic
M-211
Coleridge
Longfellow
Double tape (Pagoda)
Alb
Scramb
OTP

65
66
196
1961

LECTURE NOTE For principal operations of COMINT

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

(104)

Let's dispose of T/A first.

T/A is very important for two reasons

1) Establishing networks when call signs & frequencies change frequently, as in case of German Armed Forces

2) In absence of decrypts – is highly useful & may be the only source of COMINT

Show slides of RFP & Morse Op Ident { 255, 256, 254

Information from abb & flow of ltfc – 238, 239

Read from "All honorable men"

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.

(over)

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 proportions of supplies and

(See 238-3)

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.

End 238

REF ID:A38356

RFP

I
II } Two different transmitters

254
255
256

TINA N Morse Operator Identification

Stop! Don't click — Next 2 cards

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 repetions between and within messages.
5. Preparation of statistical counts of letters, grps.e
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, isolegs, homologs
10. Reduce to simplest terms.

(105)

LECTURE NOTE

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

LECTURE FOR SLIDE 245 ~~102~~

Trithemius
~~Collange, Gabriel de~~

(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.

If time permits - tell Semiramus story

(102)

LECTURE NOTE FOR SLIDE 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

LECTURE NOTE

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

Navy began using IBM ~ 1932

Combined total (1934 1945) - 750

Now in NSA (1954) — 314

(108)

135

Extract from 1st Contract with IBM

Tell how — got it put over —
AMG's Office had IBM installation
for CCC accounting —
Cancelled when an old-timer can't
see any new-fangled notions

LECTURE NOTE

One wing of IBM installation in WW II

(110)

The basic and most important analytic machines we had were those for German Enigma
The Navy Bombes — 90 sets of 4 high sp com each running at 1800 r p m
The Army Madame X - Electrical relays
Regret I have no slides to show of those
Explain why

Geheimschreiber

150,150.1

The Japanese "Purple" - our version

Two slides.

LIGHTS ON

(119)

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

---

70 mm Comparator was 1st machine
Built in late 30's by Bush MIT, put into
service 1942 85 letters/second

Copperhead - to search for 2-group hits in sum pl
code. Put into use in 1944 — now obsolete with
701 Computer

253 - Alcatraz - monographic & digraphic frequency counts
145 - Machine decipherment
137 - Locating repetitions - "Brute force" machine
138 - " " - "Slide rule"
139 - Another machine for decoding & deciphering
140 - CAMEL - Clyppen
145 - " Code indicator locator
194 - Assembly of components
200.1 - JAS decipherment
201 - Selective J-square
202 } J-square permutor
2021 }
142 - Purple dudbuster
199 }
199.2 } SIGEE additive generator (typing) — over —

143.1 - Auto scratcher (Rodin)
198.1 - Geheimschreiber code tester

248 - O'Malley - Specialized arith computation - gives determinations of products of pairs of numbers

249 - Demon II

250 } Goldberg - Concordance machine, general purpose
251 } large scale. Fast - NSA one
with magnetic drum for storage

259 - Atlas

New machines —
CONNIE I - teletype scrambler - 5000/sec + print
II - greater reliability
VIVIAN - comparator using mercury delay line
DELLA - 5 million comparisons/sec as against Robin's 5000

LECTURE NOTE

A "brute force" machine

(114)

LECTURE NOTE

Machine for matching messages

(115)

LECTURE NOTE

The "Auto-scritcher"

/Rodin - the "Thinker"/

(118)

LECTURE NOTE

An analog.

(This was for JAS system (Jap MilAtt)

(11)

248

O'Malley

Specialized arithmetic computation gives summations of products of pairs of numbers having up to four digits

REF ID:A38356

259 A

ATLAS

STOP! DONT CLICK. See next card

over [Assistance we had from By]

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 motors

c Stereotypy + methodicalness of G mind so that cribs + cross-cribbing poss passing msgs from 1 net to another without [illegible]

over -

- over -

2 Pacific Theatre
a Lack of technical know-how
b Complexities piled on complexities + dependence thereon for security
c. Errors therefore
d Methodolatry + stereotypy

3 Brilliance of UK-US crypt
→ what we owe to UK
4 Money to spend on COMINT activities

Read from Brownell Report

234

Chart showing processing steps from originator to consumer (Army)

Chart showing no. of "bulletins" 235

[illegible]

REF ID:A38356

Navy C.I. organization

Combined C.I. "

EXTRACTS FROM PART II, BROWNELL COMMITTEE REPORT
(JUNE 1952)

In World War II COMINT may well have been our best paying investment. Its cost 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 enrout

(over)

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.

Extract from the report of the Joint Combat Intelligence Center, Pacific Ocean Areas, on this engagement:

"The factors that vitally affected the Battle of Midway were many and complex, but it is undoubtedly true that without radio intelligence it would have been impossible to have achieved the concentration of forces and the tactical surprise that made the victory possible." (See 3)

In 1942 COMINT told of the critical Japanese decision not to join the Axis war on Russia (but U.S. authorities thought the message a "phony" - meant to deceive us!)

In 1944 it helped us to pick the soft spots for our island advance, often showing where the Japanese expected us to attack and where their troops were massed.

The Strategic Bombing Survey mission which checked on shipping losses after the surrender discovered that COMINT's knowledge of the size and location of the Japanese merchant fleet on V-J day had been more exact than the records of the Japanese Ministry of Merchant Marine.

See 4)

Finally, COMINT provided us with our only reliable measure of how fast the Japanese were losing their will to resist. Our leaders had a thorough and immediate record of the peace feelers which the Japanese asked Ambassador Sato in Moscow to send us through the Russians and of the explanations to him of how decisions were being reached and on what points further concessions would be made.

The principal public credit for winning the Battle of Britain has gone to radar and the "so few" to whom so many owed so much. But much credit is also due to another British "few" who rapidly deciphered the high level

(See 5)

combat traffic of the Luft-Waffe, and guided the airborne "few" to the defense of the right place at the right time.

In the war on land COMINT did even better. It read Rommel's intentions in Africa so well that the Desert Fox guessed the truth, he confided his suspicions to Berlin, only to be tol by the German High Command that such things were not possible.

Before D-day in France, COMINT furnished several of von Rundstedt's periodic appraisals of the situation for the High Command, showing where he thought the main attack would come, as well as some of Berlin's replies ignoring

(See 6)

Rundstedt's good advice, presumably in favor of Hitler intuition. COMINT also contributed Ambassador Oshima's detailed reports to Tokyo on his pre-invasion tour of the Channel defenses, which led (the Committee has been told), to basic revisions in our landing plans After the assault was launched, COMINT supplie a large quantity of battle reports and battle orders on every level from the OKW itself down to the various divisions. Throughout the campaign in France and Germany, our estimates of enemy troop strengths, locations and intentions were based more on COMINT than on any other source. COMINT was also the principal source of the information used to select

(See 7)

strategic and tactical bombing targets behind German lines; and it helped us to identify the testing of advanced weapons (such as improved torpedoes and guided missiles) in time to get our scientists started on suitable counter-measures, thus greatly reducing the ultimate tactical effectiveness of the enemy's new developments.

Protection of Convoy

As to our successes, have mentioned + read from PH Report

Now read from Brownell Com Report of June 1952

SECURITY VIOLATIONS CARD 1

from "The Memoirs of Cordell Hull," Vol. II, The MacMillian Company, N. Y., 1948, Chapter 71, "We Talk with Japan," pp. 998.

Actually, we already knew the contents of the message. It contained a statement from Matsuoka to me that the German and Italian leaders were confident of victory, that American participation in the European War would merely prolong it and bring about the destruction of civilization, and that Japan could not injure the position of her allies.

(OVER)

We knew this because of the fact that our Navy and Army cipher experts, with remarkable ingenuity, had broken the Japanese code and were deciphering Government messages from Tokyo to Washington and other capitals, translating them and sending them to the State Department for our information.

These intercepts, bearing our code name "Magic," played little part in our early negotiations, but were of great importance during the final phases. They enabled us to know many of the instructions the Japanese Foreign Minister was sending to Nomura and to other Japanese representatives; they gave us a check on what Nomura was reporting to Tokyo concerning the conversations he was holding with me; and they showed that the Japanese Government was going ahead with its plans even

(CONTINUED ON CARD 2)

while talking of peace with us. I looked upon them as I would upon a witness who was testifying against his own side of a case.

I naturally had to be careful never to give Nomura the slightest impression of this special knowledge. I had to take care to keep our conversation limited to the knowledge I might have gained from him or from normal diplomatic sources. So as to safeguard the security of these messages, I named one of my secretaries to handle them, keep track of them, and make sure they were either returned to the Navy or destroyed.

A few words re organization required for effective CI operations.

Interception of foreign communications and subsequen processing requires services of large numbers of commun ications and specially trained personnel. In order tha the product may be most useful operationally -- and not merely historically interesting, the intercept traffic must be forwarded most expeditiously to the processing center and after processing, the final results must be transmitted promptly to the evaluators and other intelligence personnel and in some cases directly to field commands by fastest means. This forwarding to a large processing center necessary now because of complexity o modern cryptosystems -- can't be solved in the field - except low grade and T/A.

(121)

Some CI processing can be accomplished in the field as I said before - in order to meet certain immediate needs of field commanders. Each service provides for its own special needs in this category but CI processi, is essentially complex activity and much of it can be done well only at major processing plants where the limited number of highly skilled personnel can be concentrated and very specialized analytic machinery can be installed and maintained. -No pool in civil occupations and must train our own very largely in all phases.

Now I come to Korea and say a few words about part played by AFSS.

(122)

Say a few words about very great importance of coordination of COMINT activities with other intelligence operations and with the tactical situation. Although COMINT is the most reliable, the most timely, and the most inexpensive kind of intelligence, it must still be evaluated, collated, correlated, and coordinated with intelligence coming from other sources -- if for only one reason alone -- to provide data for cover and protection of COMINT sources. When a decision has been made to take action based on CI, careful effort must be made to insure that the action cannot be attributed to CI alone. When possible action must always be preceded by suitable reconnaissance and other deceptive measures -- otherwise goose is killed.

Will give three examples of "cover" for COMINT:

1. Tunisia (official report) - 2 German code messages intercepted several hours apart -both solved. 1st stated intent of Germans to attack at particular hour. 2nd postponed attack and gave new time of jump-off. Both solved and sent to Allied tactical command at once. One command after receiving 2nd message made radio broadcast in clear telling story. Germans intercepted broadcast and attack again postponed. Information sent different way. But most important point: they changed all c- and Allied COMINT disappeare until new ones were solved.

This second breach committed not by subordinate, inexperienced officer but by high ranker. He got sever reprimand.

(129)

2nd example better and from same report: "On 28 March a new German unit heard for the first time sent two messages. The first at 1335, revealed 2 gun positions. At 1500 a Piper cub was sent over the areas as a decoy for the source of information. At 1600 Allied artillery began to lay down a concentration. The second message from the German unit requested an ambulance. The unit was never heard from again."

3rd example last: From Pacific Theater:
On certain day November 1944, an enciphered code message was sent bya certain Japanese staff section to certain Japanese Air Force units requesting air escort for two convoys carrying troops to reinforce the Philippines. Message gave number of ships, tankers

escort vessels, date of departure and port, route, noon positions for next 7 days; message solved in Washington. Two days after the convoy left one report in message which was also intercepted and solved that it had been sighted by a B-29 with strong indication that other convoy had also been sighted. A few hours later, messges from these convoys reported losses: 6 ships definitely sunk, one disabled, one on fire. Later we learned from another source, in addition, one aircraft carrier was also sunk. Did you notice message about B-29? It didn't "just happen" to be cruising around!

Of course, knowledge and experience point to necessity of exploiting every possible advantage a tactical situation affords and the temptation is of course very great in the heat of battle to use CI whenever and wherever it is available. This may lead to carelessness which quickly jeopardizes CI sources. Of course, full value of CI cannot be realized unless operational use is made of it. However, when action based on it is contemplated, possible compromise of source must always be borne in mind and danger of compromise weighed against military advantages to be gaine Minor military advantage is never alone sufficient grounds for risking loss of source. Also must bear in mind that cryptosystems usually world-wide or area-wide

(OVER)

in usage. Changes made as result of suspicion of compromise may have far-reaching consequences on ability to produce CI elsewhere. A commander seeking a minor advantage by using CI in one locality may deprive another commander of much greater advantages or even deny it to commander of a major operation.

Another aspect of coordination -between operations and CI. COMINT people should be carefully oriented to give optimum coverage for operations in progress. There are just so many facilities and personnel available and only a part of enormous traffic can be obtained and processed. Hence, essential that CI people be constantly informed of current and planned operatio so as direct attention where most needed. Also that information is often essential in proper interpretatio of certain material and can help in solution.

Advice against knocking out radio stations.

(128)

Re current manner of employing COMINT - can be discussed under various headings but neither time nor security rules will permit. However, it is obvious from the Pearl Harbour disclosures alone that the manner of its employment during WW II must have been quite efficacious. I started this talk by reading from TIME and now I'll come back to it to read you some more of the Marshall-Dewey letter because that will give you a pretty good idea of the contribution COMINT made toward our winning WW II. You'll recall that TIME mentioned something about a machine which it called "Magic". Here is a picture of it --last slide! LIGHTS ON.

(120)

[illegible] that everyone of you has had -
experience more than once in the last few months It goes like this. You're in bed trying to get to sleep You've had a bad day at school and things were a bit difficult To begin with you didn't feel so well when you woke up early from a disturbed and restless sleep - so you were dopey all day and drank coffee or cokes to help you through the day But now the caffeine is having its effect and you can't seem to fall asleep even as tired as you are Things begin churning in your mind What was it that VIP said about our being an easy target for a surprise air attack with A- or with H- bombs?

Who was it that told us our radar fence protection was ridiculous Our ADC could at best knock down - what was that figure? - at most 10-15% of the bombers carrying the bomb Yes, and now look at all these columnists comments on the reports of these special study groups set up to

inst a knock-out, sudden attack Let's see: there
s the Lincoln Summer Study project at MIT It's report
ared the daylights out of certain of the high brass in
shington So they appointed another group to evaluate
e Lincoln report - the Kelly group The Kelly group
rned in a report that seemed to be so shocking that it
s practically been suppressed Then the brass appointed
group to study the Kelly report - the Bull Committee set
p by the NSC (Read extracts from Alsop)

Well, now sleep has left you for good because you feel
retty scared - not on account of your own skin - but what
bout the gal who's asleep beside you and those kids in
he next room? No wonder you're scared and you're worried
hat thinking American isn't these days? And we recently
earned officially they have set off an H bomb What to
o? Well, cheer up a bit. There's one more possible

answer that the Lincoln, Kelly, Edwards, Bull and Black Committees didn't get - because they weren't let in on a certain very secret. It's that very secret I'm going to talk about this morning. It's name is COMINT.

for the rest of my lecture

Now I don't want you to think that COMINT played no part in the recent Korea Police Action. I'll come back to that in a moment or two. Before doing so I must say a few words on the subject of the general types of organization for effective COMINT operations.

Extract from: Citation for 1st Radio Squadron, Mobile for Award of Meritorious Unit Commendation in Department of Air Force General Order 64 of 11 Oct 1951

"The contributions of the 1st Radio Squadron, Mobile, in direct support of the UN combat effort in Korea have furnished the UN Forces and the Government of the United States with tactical and strategic intelligence, of incalculable value to the success of the UN mission and to the security of the United States, and have thereby reflected great credit on the unit and the Air Forces of the United States."

With these last remarks I bring to a close the series of talks on History. I've been invited to stay on for a couple of weeks, to participate in SCAMP activities in whatever way I see fit. I plan to sit in on certain presentations by other participants in this symposium; but I shall be available to any of you who may wish to talk with me individually on cryptologic matters

- over -

or on activities of NSA This I will be very glad to do Also, if any one of you wishes to examine and discuss any of the books and exhibits I have with me, I shall be glad to do so.

Thank you very much for your patience in listening to my rather lengthy talks and for your courtesy in paying such careful attention to what I had to say