Transcribed
from tape,
SCAMP 58

Lecture VI
Section 1

Gentlemen, we will begin the final session in my series of talks. It will be

devoted to four main topics First, what sort of codes and ciphers were we

confronted with immediately before and during World War II? Second, what

were we able to do with them, and how did we do it? 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? Finally,

what are the prognostications for the future?

Let's begin with the first of these four topics What codes and ciphers,

or more technically speaking, what cryptosystems confronted us immediately

before and during our participation as a belligerent in World War II? In the

European Theater, there was of course the problem of tackling a multiplicity

of pretty high grade cryptosystems of the Germans. Take first the diplomatic

ones of which there were two very high grade systems   One of them we

called by the code name, which the British used, FLORA DORA   It consisted

of an additive system, applied to a basic codebook with numerical code groups

was a very good one.

The code group was large to begin with, and the additive system, I think you

the designation "additive" —

all understand what is meant by that, you add numbers from a book or list to

the resulting number

the numerical designations of the code groups and that then becomes the

In some systems you do subtraction instead of addition.)

enciphered code text   In the FLORA DORA system the Germans had two separate

and the two books were used in combination.

additive books, each one consisted of 10,000 five-digit groups   You can see

That is, one could

that this produces a large number of groups when you can take any one of the

5-digit groups from one book   in that book

10,000 of one group as a starting point and anyone of the 10,000 groups of the

in that book; these two groups

second book as the starting point and these are added together and the sum of

From these starting points one continued in the
same manner to decipher the rest of the code groups
of the code message to be superenciphered.

the two additives is then applied to the code group ⋀ ~~We were able with the~~

Together with
~~help of~~ the British *,* ~~collaboratively~~ *we* read most of the messages in that

system

There was another high-grade system used by the Germans which was a one-

time system, so called Everybody thought it was a one-time system. By this

I mean a system of the sort which I have just described but using the additive

once and only once Now these messages passed from Berlin to all of the

diplomatic posts abroad in quantity by radio and for a couple of years the

messages were simply put aside They were considered hopeless They gave

every evidence of being in a one-time pad system One day a man travelling as

an ordinary traveler, passing through the Panama Canal, was questioned and

there was reason to suspect that he might be a German secret agent Secretly

his belongings were searched and sure enough there were discovered among

those belongings some one-time pads which he was carrying for some destination

These were separated from the gentleman in question and were brought to

Washington. They were set aside too because they gave every evidence of

being the ordinary sort of one-time pad--you use a page, tear it off, and

burn it after you have used it But there happened to be one or two people

in Army Security Agency at that time who looked at these pages of pad additive

rather intently for some time and they came to the conclusion that those

additive groups were not made by some random action, machineof some sort

using electronic noise It was soon apparent that the pages of additive

were derived by the action of some sort of machine which gave evidence of

-2-

being a generator of one sort or another   To make a long story short we

discovered the way in which this machine operated to produce the groups on

each page but there remained one difficulty   It seems that the Germans in

making up these pads had the machine print these pages in duplicate and these

pages, single sheets, were then put on a large table and somebody went around

and took a page from one pile and then a page from another pile and just

walked at random over and over--what you would call a random-walk in mathematics

and in this way the pads were made in duplicate   What was the problem then?

We had been able to reconstruct the machine but how to find out which page of

a given stream of characters or groups was used for a specific message. We

developed a machine for taking a message and passing the code groups of that

message against the product of the machine generator at a very high rate of

speed and determining in this way the page that was used for the encipherment

of the code groups of a specific message   This involved a lot of work but

it paid great dividends   We were able to read pretty nearly all of the

messages after the elements of the system had been reconstructed

After the war was over, and we had teams going around following the

victorious armies, we captured some records of one of the cryptologic agencies

of the German forces and there we found a complete description of this

machine   Curiously it had been offered by the manufacturer for sale to the

British on the open market sometime in 1935

We come now to the cryptosystems employed by the Armed Forces of the

Germans   There were low-level codes, I think we could start now with the

first slide   That's an example of what was called the ALKA, an Air Force

system   I won't go into that   It changed everyday but through careful

following the codes were read from day to day

Next they had a system called the double PLAYFAIR   I won't undertake

to go through that--it is a little complicated, fairly secure, but most of

the traffic in that was read and they had a thing called RASTER, "Rasterschluessel "

It was a matrix with holes in it, disposed randomly and you had to know where

to begin   There was a key, an indicator, and you began a certain place and

you wrote the letters of your message in the open spaces and took them out from

columns and the roster changed very frequently--I don't remember at the moment

if it was daily or not, but it changed very frequently   We didn't have too

much luck with it   It was a pretty complicated thing but it was used for the

medium level communications

Then, of course, we had the ENIGMA, used by the Army and the Air Force--

a three wheel machine, I think I showed a picture of that with the plugboard

or stecker as they called it   The Navy version of the ENIGMA was a four-wheel

machine and toward the end of the war, when the Germans began feeling a little

bit uneasy about the ENIGMA, they proposed to make a reversing wheel which

would   , that is, the 13, the 26 contacts in that reversing wheel could

be plugged at random and changed daily or more often   This we called UNCLE DICK

and was a very serious threat but the war came to an end before they actually

got the thing going

Now the Germans also had a series of machines which went by the general

codename of the fishes   The first such machine was called TUNNEY   It was a

teleprinter ciphering machine and they called it the HANDSCHRIEBER. There

were about five different models progressively increasing in complexity   They

were solved at the beginning as the result of finding of messages in depth,

that is, the setting points, I think this is, oh, that is just a German key

list for the ENIGMA--they had many of those captured   This is a HANDSCHRIEBER,

a rather complicated looking gadget   I won't undertake to go into it but we

read a good deal of traffic in that particular machine and its descendents

The Italians didn't count for very much   They had codes, codebooks and en-

ciphered codes   By the time our forces were in direct contact with the Italian

military forces, they were pretty well disorganized and what there were in the

way of secret communications were German--ENIGMA

In the Pacific Theater the Japanese for their diplomatic systems used

simple codes, one for, purely for, economy purposes   Another enciphered code

using a basic code which was changed   every so often and the code groups of

which were then subjected to a transposition and the transposition key changed

daily   We were able to keep up with that particular type of system   Just

before the war, our participation in it, the Japanese Foreign Office used

a machine which we called the RED   It was a cipher machine   Oh, I forgot to

tell you about that one   That was the German SG-41, a machine which they

proposed to put into use but never actually did   I doubt very much if there

was any traffic   They stole Mr Hagelin's ideas and had a fixed pinwheel and

a cage with sliding bars   What they added was a keyboard and the printing

mechanism   It was a tremendously heavy thing, very unwieldy and I don't think

think they could have operated it successfully

This is what we used to read the Japanese diplomatic messages in the RED

cipher machine   We never did see a RED machine   It was reconstructed, the

system was reconstructed without having knowledge of its actual physical

                                                                    means of
embodiment but we could duplicate what the machine did by/a celluloid disk

which was stepped irregularly going to certain keys   I think that this

picture represents the Japanese Navy version of the RED cipher machine captured

sometime shortly after the war was over

Then the Japanese had, well that is the Navy's equivalent to solve the RED

Japanese XXXX Naval Attache messages--this was the Navy's version of their

analog

We come now to that famous PURPLE thing used by the Foreign Office for

its highest level communications   You all know that the basis for the solution

of ciphers is the principle of frequency   Frequency of the use of letters,

characters   This means that the distribution of the characters in normal

plain text is not homogenous, it is rather ragged, high spots and low spots.

Now, the Japanese who designed their machine figured that since fequencies

were the keystone of cryptanalytic solution, they would build a machine which

would suppress frequencies in other words, within a certain length of text,

it was impossible that any letter could be represented by the same cipher

equivalent   This means that in their PURPLE machine which was a 26-character

machine, in every line of 26-letters of text, there could be no dual ortriple

representation of the same plain text letter. This was the fatal flaw   This

is what enabled us to get our first wedge into the system It was soon after

that this phenomena was discovered that we were on the trail and we had some

help from cribs that consisted of portions of text that we felt would be

found in Japanese diplomatic notes to our Government The work was slow and

painful, very arduous This was done by the Army crew and there came a day

when we had about exhausted our resources We had recovered some several

hundred letters of text and it made sense but at the end of that period there

was a series of messages which appeared to me to be the English text of a

long note which the Japanese Government had handed to our Government, our

Secretary of State, dealing with the announcement of the Economic Treaty

that had been in effect for several years The Japanese were very anxious

to have that treaty kept in effect Well, I worked with my colleagues on the

messages and I came to the point where I felt pretty sure that there was a

message and it must be in the Department of State's files. Now, at that

time, we were under very strict instructions not to go ourselves to seek

collateral information but always to work through a designated representative

in G-2 and I went to this chap and I asked him to look for a message, such and

such a date dealing with the Economic Treaty He said he would A couple of

weeks passed by, I didn't hear from him. We were struggling with the thing

We would get maybe half a dozen letters out in one day's work I asked him,

well, what about that message? And he said, there is no such message Well,

I felt disheartened and went back to my lair and continued to work, a few more

letters, another week, and I became a little bit more sure that there must

be such a message so I went to him again and I said, "Major, will you please

check and verify that there is no such message " And he said, "I'll do that "

And a week went by and he didn't come to see me I went to see xkxkx him

"What about it Major" -- "I assure you there is no such message" Well, I was

very much disheartened but I went back, assured my people that we ought to

keep gong, it was important Reluctantly, they continued and we got a few

more letters. By that time, I made up my mind that there must be the message

so in violation of my very clear-cut instructions, I went myself to the Chief

of the Communications and Records Division of the Department of State and it

happened to be a friend and I sat down. "What can I do for you today"? "I

think there is a message here which I would like very much to see in your

files " He said, "Well, if it is here, I will be glad to try to find it

Give me some data " I gave him the date, subject He pushes a button and

this girl comes in and within two minutes, that book with the text of that

message was opened before me And I said,"Dave, I need this " He said,

"You know what my instructions are, you know you can't have it," I said,

"Dave, for goodness sake, don't you have to go out to the can " He said, "Yes,

by the way, I do" I copied the message That gave us an xxx awfully great

push forward From then on we were well on the way We constructed by hand

a very simple device which we could use to duplicate the workings of that

machine, fairly complicated I have shown you the front of it, back of it

full of wiring We never did see a Japanese PURPLE machine They were

destroyed by instructions just before the attack on Pearl Harbor The only

thing we ever did see was a very badly beaten up machine burnt and so on in

the basement of the Japanese Chancellery in Berlin. Oh, we did have a few

pieces I don't know whether I should tell this or not After the Army

and the Navy got together and played in the cryptologic garden, there came a

day when we had reconstructed this PURPLE machine and then I had a telephone

call from the Head of the Laboratory of the Federal Bureau of Investigation and

they had a cipher unit too He called up and said, "I got something here that

might interest you" I said, "Well, I'll come over " So I went over and he

told me this story in his office That on the day of the attack on Pearl

Harbor, a couple of their operatives were watching the Japanese Embassy in

Mexico City and a couple of Japanese gentlemen came out carrying two suitcases

and they got into a black limousine and they dashed off to the city dump The

operatives followed as closely as they could and watched The Japanese put

something on the city dump and returned to their automobile and after they

had left the operatives went to see what there was and they came across a

large lot of parts that had been pretty badly beaten up and they assembled

them, shipped them in a box and they are in the next room, he said I put

them on the table. Well, I went there and I took one look and I saw that it

had the type of stepping relays that were used in this Japanese PURPLE machine,

it must have been We had to duplicate the relays, telephone relays

and there I was confronted with a problem What to say? Well, I stalled, went

back and we had a little talk with our friends in the Navy and this is what

we decided to do. The FBI was very anxious to reconstruct that machine. We

were very anxious that they not so we sent two men, one from the Army and one

from the Navy, our very best technicians, to make sure that they didn't put

it together properly

Question.

Well, they had no functions in the field of diplomatic military communica-

tions Their functions were purely in the area of domestic counter espionage

and we thought that they should stick to their knitting. They did, as a matter

of fact, after we had an agreement worked out but among us, the three organi-

zations

Now, so much for the Japanese diplomatic people When I opened my talks

I read you something about the meaning of the solution of that thing This

is our reconstruction after we got underway This probably doesn't look at all

like the Japanese machine did but that's our reconstruction I think maybe

there's another picture--shows some of the wiring in the back--there were three

sets of equivalent to commutators

Now we take up the Japanese military things The Attaches had an enciphered

code, a complicated thing You remember my telling you about how we were very

much discombobulated when the OSS without authority or rather without the

knowledge of the military and naval authorities made that raid in Lisbon and

put us out of business for a while. The Naval Attaches used a machine I think

that that has something to do with it--well that was the machine, the set of

machines that we used, to read the Japanese military enciphered code systems

We always tried wherever possible to reduce these hand-operated systems to

machine operations so that we could save time and people The ground forces

had proposed to use a machine that we called the GREEN. It was captured

in action and shipped to Washington immediately. It was on field testwhen

it was captured   And we decided that if they were going to use the machine

we ought to get ourselves in position to decipher messages in a hurry   There

is the keyboard for that thing and so we built machinery to solve GREEN cipher

machine messages if they came in   None did   The machine was not successful

It was really a very poor piece of engineering   The Germans furnished the

Japanese with some ENIGMA machines and we thought for a while that they were

going to go in for ENIGMA and fortunately they didn't   ~~Theyxxmmkd~~ It would have made

life a good deal more difficult to be confronted with that

      The Japanese Navy used--well, that is a code, a Japanese code which was

used by the Ground Forces and they enciphered it by complicated gadgetry, I

mean complicated hand-operated things, additives and they disguised the

indicators--I used the word additive, I shouldn't have because they didn't

actually after a while use the code groups as additive, they used the code

groups of the keying table as key groups to encipher them by means of a square

of this nature   so on.

The Japanese Navy used a system which was an ellaboration and quite an elabora-

tion on the strip cipher, called the JN-25 and to the glory of our Navy, they

were up on top of it most of the timeexcept when somebody spilt the beans

and would publish something like how Midway happened to be won and that sort

of thing   I think Marshall Hall could probably tell you a good deal about that

and also Dr Tompkins would have more direct contact to that than I. I mentioned

-11-

the Japanese Naval Attache machine which was a good deal like the PURPLE.

AS long as we are talking about machines and enemies, we might as well talk

about some of the machines used by the Russians.

In the first place, Russian traffic nowadays is difficult to identify,

I mean by that externally very often you can't tell from the message itself

whether it is Air Force or Navy or Ground Force or diplomatic   It's all one

so you have at the very beginning a problem of isolating the traffic into

systems   Now soon after World War I was ended, the Russians built a machine.

There I show you the old B-211 of Mr Hagelin's, the Swedish inventor and this

is the inside of that machine which I showed just immediately before   I want

                                                                          are
you to take note of cave, that is with the sliding bars and here xx the

commutators, these are not actual rotors that were used in the ENIGMA but

they are somewhat like rotors   What the Russians did was to build a machine

copying that B-211 and modifying it only to the extent of making it a 30-

character machine instead of the 25, which the old Swedish machine was and

                 box
they added a black/to the side so that they could change the connections to

those commutators   That machine was in use for about a year or so--we had

no difficulty with it   There were other systems that they used which we were

fortunate to find answers for--one called COLERIDGE and one called LONGFELLOW,

OUR COde designations   They had one which was of particular interest to me.

It was called PAGODA and it was a teleprinter enciphering system which they

had copied absolutely, literally from a paper which was published in the

Proceedings of the IRE in 1922   It was a double tape system just exactly like

I showed you in one of the slides yesterday where you had two tapes revolving, producing by their inter-action a key which was then applied to the text--the plain text

Now, the Russians even with that very simple system couldn't work it. In the first place, they gave lots of depths and in the second place, after they found they couldn't work xx two tapes, they worked one tape and they couldn't even work that and they had many, many depths   They gave it up. I imagine that they had some people studying their cryptography xxxxxxxxxx intensively because it wasn't very long before we found ourselves up against some very difficult things. They studied hard and they have produced something which thus far is quite baffling   They use one-time pads   At one period of their history, they used these one-time pads twice--this is   What they did was to use say pad 14 between Moscow and Buenos Aires in September to December 1944. Now that same pad would turn up, say three or four years later, 1957 between say Moscow and Ottawa   The trick was to find the double use   Why they used a book, a pad, twice and not three times, I don't know and nobody can give me the answer to that   So far as our investigations have gone, they never used one more than twice and sometime in 1948, 49, I forget now, the double use ceased and we have since then not even been able to prove whether they are using them twice   Dr. Engstrom mentioned the SCRAMBLER problem and the difficulties we were having with that and the immense amount of money that it is taking to get into these high-level Russian things. Of course, if war should come and it shouldn't be over in ten days or twenty days, the Russians

would not be able to operate their one-time pad systems because we think, we

hope, that they would not be able to get new pads distributed   There is a

limit to the number of pads that you can store and therefore they would have

to use something else.   At the moment the Russians have not any one of their

two important cipher machines anyplace outside their own territory with the

exception, you can call East Germany their territory I suppose   There is

something in Berlin but that is all   They don't use their machines for

communications abroad.   This does not necessarily mean that they don't have

them.   They might have them in readiness but nobody can tell

Now, I'm going to--I think that's the end of that series, let's see--well

that's the inner workings of that M-211, as we called it, the Russian machine,

I think that's the last of the series

briefly
I'm going to talk generally about some general principles and then we will

have a break and then we'll resume   Now some of this will be "old hat" to

some of you but for the newcomers, perhaps it's wise to mention the principal

operations upon which communication intelligence activities are based.   First,

of course, there comes the intercept--you've got to have the material.   This

is no small trick   The modern electrical high speed communications require

high-speed intercept operations and together with the intercept, there must

bedirection finding, when you are working on the communications of armed

forces of a government   The Russians, for example, have complicated callsign

systems, complicated shifting of frequencies, so that it is important to be

able to identify transmissions either by direction finding or by one of two

other types of operations   One is called radio fingerprinting, which simply

means that every transmitter emits electro-magnetic radiations which have

characteristics that are analagous to the characteristics of a fingerprint and

it is possible therefore to identify a transmitter by studying the characteristics

of its emanations   It is also possible to identify a hand-operated Morse

telegraph communication   That is, every operator has characteristics of his

own hands and wrists and you can by studying the transmissions of Morse

operators, identify them.   This is very useful   Much work remains to be done

in Direction Finding, in Radio Fingerprinting and in Morse Operator Identifica-

tion.   I think that that slide I cut off is an RFP test   shot showing a

recorded transmitter and one that you have in the record and compare it to a

new transmission to see if the shape of the waves is very very similar   There

is another one.   Here is Morse Operator identification   dots,

the length of dots, the difference between dots and dashes and lengths of

dashes, the characteristics of each operator   (Now cut the lantern off, I

think we will go on for a moment.)

The next step after interception is traffic analysis, that is, the

reconstruction of the radio nets of the enemy and the location of their

transmitter stations   This gives very important information on two counts

First of all, establishing or reconstructing the nets gives you order of

battle which is very important.   The reconstruction of the networks is not an

easy thing for when the callsigns and frequencies are changed rapidly   It is

a curious thing that the Germans seemed to be able to change their callsigns

and frequencies without too much trouble--it gave us and the British a good

deal of trouble to begin with   We had to keep people working at it all the

time but I contrast that with the situation in our own Armed Forces, our ground

forces at least   It has not been possible to get our Army to adopt a sensible

system of callsign changing   They say, you will either have communications

or you will have callsign changing, you can't have both. When it is pointed

out to them that other armies do it and have done it, they have apparently

no answer   The Navy changes its callsigns and changes its frequencies--maybe

their problems are a little bit less difficult/

Now the second good reason for engaging in traffic analysis is this.

Every once in a while your cryptanalysis meets a roadblock and you don't have

any   You don't have any COMINT from decrypts so the only thing you have to

fall back upon are these other sources of information, aerial observation,

pictures and that sort of thing but traffic analysis from simply watching the

ebb and flow of traffic and the direction you can make inferences of what is

going to happen. Now these, mind you, are inferences -- they are not right

out of the horses mouth as decrypts are.

The next step, of course, is cryptanalysis   Solution of the messages

and, if they are in foreign language the translation and with the translation

there is always a certain amount of ᵗʳᵃⁿˢˡᵃᵗⁱᵒⁿ emendation, you've got to make corrections

Errors in transmission, errors in reception, erros on the part of the cipher

clerk and so on. Then the next thing is large scale production or exploitation

You are not dealing with single individual messages a day--there are

thousands of them   I"ll show you a graph later on--what this means.

The next step is the evaluation of the information and mind you, I've

been talking about the COMINT product as information. This is something which

the intelligence people are most insistent about   The COMINT people don't

produce intelligence they say, they call it information, communication

intelligence information, if there is such a   expression   It's

their job to evaluate it and to collate it with information from other sources

to check it and that sort of thing. And I suppose that this is a very

necessary thing.   It is conceivable that an enemy, an astute enemy, might

actually mislead you by sending out a phoney or two in which case the intelli-

gence people should be able to detect this character by collating what it

says with what it has from other sources

And then there comes finally the dissemination of the product and this

has to be very very carefully controlled.

Now, I think we have reached a good stopping place and we will have a

break of about five minutes, no more, as we have a good deal of territory to

cover and we want to finish here by 4.00 6'clock at the latest, I'd like to

make it 5 minutes to 4:00 so that those of you who want to attend the other

talk will have time to walk over to the building.