Oral History Interview

NSA. OH 01-74 to 12-74

with

Mr Frank B. Rowlett

26 June 1974
(and subsequent dates)

National Security Agency

By: Vincent Wilson
Henry Schorreck
David Goodman

Declassified and Approved for Release by NSA on 10-21-2021
pursuant to E.O. 13526; MDR 80299

INTRO: Today is 26 June 1974 Our interviewee is Mr Frank B Rowlett, a renowned cryptographer whose career ~~is~~ dates back to the mid-1930's. He joined the Signal Intelligence Service at the Munitions Building in Washington, DC and served with successor agencies - the ASA, AFSA and the National Security Agency until his retirement. Mr Rowlett will discuss his career as a civilian with the SIS and as an Army officer with the Signal Service Agency during WWII. Interview is taking place

(over)

at NSA, Fort Meade, Maryland.

Interviewers are Vincent Wilson, [redacted] Henry Schaneck and David Gordon. The classification of this interview is Top Secret. Handle Via COMINT channels.

HANDLE VIA

FBR Do you want me to start with April Fool's Day 1930 when I came to work, or do you want me to go back into of that my what I did in college and high school? Start Sort of from the cradle to the grave grade thing, Or do you, I mean, I can do either one, of them.

I (Wilson) Well, let's take the education, and Let's start let's say with your college The role of the education that, kind of, now looking back on it, knowledge and that kind that helped you prepare you for being here... A cryptanalyst.

FBR O.K. [In high school you, as I recall, I knew you won a lot of prizes and things like that. I know you're not you aren't going to mention those.]

start this sentence on next line (laugh)

FBR → Five of us in high school. How can you win a prize in high school with only four competors Competitors ?

It's like winning the Middlesboro art show

Slight one in the middle were our show. Let's start with the things I think helped ed me to become a cryptanalyst. [Fine. Fine.] Q. more to separate this

Probably the most important thing was when I was a kid, I had a great admiration for Thomas Edison. And When I was about 10 or 11 years old, well, I wanted to become the greatest inventor in the world, you see. And I wanted to be able to do the things that Edison had done except much better than Edison, So this was a kid's ambition. The result of that was that I spent a lot of time learning. and I had to do this mostly from books about electricity and magnetism and the kind foolish things that kids play with, Except I got to be pretty sophisticated. because I'd buy magazines like the old Electrical Experimentor, and I'd read the Encyclopedia Britannica Wherever there was any information about electricity and magnetism that I could absorb, I absorbed it. The result of that was, that when I went to college, that but I probably knew do as much chemistry 'cause chemistry ... I'd read college textbooks in chemistry. I had a little laboratory that I'd set up myself. My dad was a very generous man

TOP SECRET HANDLE VIA

and my mother was doubly generous because if I needed money to buy some kind of a chemical or other things, a bunch of batteries, or what have you, she would find some way of getting that money to me and encouraged me to buy them. Also, my dad had a general store and the traveling salesman that he dealt with was a very good personal friend of his, ~~and~~ I could get chemicals that I needed for ~~any~~ my experiments, you see, ~~so~~ simply by telling the traveling salesman about them, and he put them in and bill~~ed~~ them to my dad. It never amounted to more than 2 or 3 dollars a month, but my dad didn't seem to withhold or have any desire to pull back on the expenditure of that money. Of course that's the only money -- there was no money -- There was no such thing as an allowance in those days, so this was his way of sort of taking care of his son's interests. With this background of ~~I got~~ an experience -- sort of self-generated -- When I got to college I automatically fell into the study of sciences and it was my ambition to become a chemist. So I lined up for scientific study in this small Virginia school aimed at becoming some kind of a chemist, and I didn't really know or care what kind. And for the same ~~same~~ reason that I chose chemistry, my background, ~~the~~ this self-induced background in electricity and magnetism led me into physics, you see. But most fortunate for me was the fact that there was a very wonderful man that I admired greatly. His name was Matthew Miller. He was the head of the math department in ~~the school~~ this little - Emory and Henry college down in Emory, Virginia and I started studying under him and, come the second year, I changed my chemistry major to a math major but I continued, and I ~~dealt~~ wound up with four majors: ~~A~~ a major in math; ~~A major in chemistry~~; a major in

HANDLE VIA COMINT CHANNELS ONLY

physics, and a major in Latin. The reason I took Latin is because when I went to college from high school ~~f~~ the high school was not an accredited school, I had to take entrance examinations in English, math, and language, which was Latin in those days, and history. Well, I did the English and the math and the history, but I had so little confidence in my knowledge of Latin that I sort of declined to take it and the fellow, the generous professor who was a real old man known as King Jimmy Cole, Professor Cole said, "Young man if you will take Latin we'll give you a conditional. You ~~practice~~ passed the other three. If you will take Latin in your first year and successfully pass it, why then we will admit you to the college." So I studied Latin because I didn't want to take the Latin entrance examination for college. Now I think these particularly well, all four of them -- I don't know which was more useful to me, but the Latin certainly gave me a feeling for word structures and how you put words ~~into~~ END TO END ~~and~~ that I'd never would have gotten from anything else I'd studied -- and I did. I had six quarters of Latin. ~~And~~ That I found most useful, particularly when we started working on foreign languages and the development of the statistical information which is useful in cryptology from a foreign language. I don't think ~~it~~ this is probably appreciated as much, routinely, in considering candidates for cryptanalysis ~~is~~ now as maybe it ought to be, because a certain understanding of languages and how languages operate is one of the things you have to develop to become a successful cryptanalyst. Maybe Latin was a useful route for me to follow. Maybe there are others for other people, but I found this one useful. I don't think I have to say much about the advantages of math and the physics

TOP SECRET

was an extremely useful thing because I think in the days when I was working actively in cryptanalysis there were very few people who had an understanding of things like relays and circuitry and switching and, as a consequence, they were pretty much overwhelmed by the complexities of electrical ~~circuits~~ circuitry and mechanical actions simply because they hadn't studied them and weren't prepared for them. ~~And~~ I think this helped me in the work we did on machines because the physics, the study of physics and the study of mechanical actions took ~~a lot~~ of the mystery out of ~~the~~ a ~~en~~cipher~~ing~~ machine. ~~becaus~~e It made sense to me because I could understand what was going on. ~~and~~ Most people who were in cryptanalysis, it didn't make sense because they didn't understand the simple pass of circuits and how relays are operated and things like that, so they were just turned off before they really got into the subject. Q. [Their circuit? the switch? They were turned on.] They didn't get turned on. Well, Vince and his puns, but still it was a four-wheel device. Now chemistry didn't do me so much good, but probably was one of the reasons that I was choosen because when Yardley had to ~~was~~ close up the "Black Chamber" one of the things that was important in intelligence was the development of secret inks. ~~And~~ I think sort of when Friedman, who selected me from the civil service registar for being hired, looked at that major in chemistry and said, "Well, this is a real good combination here. There's Latin. There's physics. There's chemistry and math." ~~And~~ I think I got hired maybe not because of my grade, but just because of the accident of these four majors that I had. ~~and~~ I think maybe Friedman was real

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

clever in using this approach because we have found in the later days that math is a good background subject for development of a certain type of cryptanalyst, and we also know that language is an important thing. Now how did I get in the government. You don't just go to college or didn't just go to college in those days and then become a government employee. I had planned to go to the University of Virginia and study math. I had a fellowship offered to me at the end of my senior year and this was through the ~~generosity~~ generosity of Dr. Miller ~~who's~~ whose son was the head of the electrical engineering department in the University of Virginia, ~~and~~ Dr. Miller had a very close connection with the University and usually his candidates for the scholarship were accepted. It was a very great thing. ~~He~~ You got 400 bucks a year and that was it. But I could get along on 400 bucks a year and go to college. The only trouble is that we didn't have too much money in our family and I wanted to get married. ~~and~~ So I was a little bit uncertain as to whether I really ~~wanted~~ wanted to pursue ~~in~~ an academic education or ~~an~~ an academic occupation like teaching which was about the only thing inside if you were a mathematician in those days. Well ~~because I was~~ being a little bit intrigued by the whole field of mathematics I saw an announcement, just about the time I was being graduated from college, about a junior mathematician's examination that was going to ~~given~~ be given in early August by the Civil ~~Service~~ Service Commission. ~~And~~ A junior mathematician at that time paid $2,000 a year which was pretty good salary. Well I had no idea that I could pass this thing, but I liked challenges of that nature. ~~So~~ I decided that I would make an application and take

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~TOP SECRET~~

the examination just to see how I would do. Really do I ~~cannot~~ CAN I compete in the field of mathematics because you look at the other students in the ~~cals~~ class around you and you say well, this is about our rating. Well, I could judge myself in terms of the other people around me, but I had NO measure of how I would stack up ~~to~~ against -- let's say a greater domain from which you take a sample, and ~~seemingly~~ seemed to me like the Civil Service examination, which was pretty well nation wide, was a pretty good way to find out ~~if~~ whether I had any prospects as a mathematician or not. So I decided to take the thing and I got the examination, the papers approving my application for it and I took this in ~~Littlesburr~~ Middleburg, Kentucky. It's an amusing thing and I remember this ~~stay~~ day very well, ~~because~~ It was a real hot day in August, and the examination had to be given by the post master because this was the only way that the Civil Service could get the examinations administered... ~~Just~~ was through some ~~govt~~ government agency. ~~and~~ The Post office of course was the most convenient one for them throughout the U.S., and the Post office in each instance served the Civil Service Commission as a place where the examinations could be taken. Well, the post master in Middleburg, Kentucky had never given one of these things and he read the instructions and he concluded that I had to: (1) spend ~~XXX~~ four hours, which was the limit on the examination, taking this; and (2) I had to be locked up in a room for this period of time. So he put me in there at 8:00 ~~and~~ in this room in the Post offic in MIDDLEBURG, Kentucky, gave me the papers, almost physically searched me to make sure I had no notes on me, locked the door and left me alone with no access to any kind of facilities like drinking water or other things that you need on a hot morning in August. I

TOP SECRET

got/
through the thing, at least all I knew how to do, in something less than 2 hours because it was pretty straight forward examination. So I sat there a ~~vurtical~~ VIRTUAL prisoner until he decided to come check on me ~~about~~ almost at lunch time. ~~and~~ ~~it~~ was hot in that room and ~~I~~ ~~guess~~ I guess I'll remember that as long as I live, as being a very uncomfortable situation. There's a little ~~better~~ brighter side to it because evidently I did pretty good. I came out ~~#3~~ number three on ~~it on~~ the register when they published the names. ~~and~~ I guess it was an easy examination because I didn't know that much math, or I was just terribly lucky. ~~And~~ Am I going in to too much foolish detail here? (No.) Well, let's do another little bit of a personal thing then. ~~When~~. Right after I'd taken ~~an~~ the examination, my wife and I decided that it was high time we got married. But I needed a job, so I accepted the job as a math teacher in a small town in southern Virginia... Rocky Mount High School. I taught math and chemistry, and I got this job and it paid less than $1,000 a year. She was teaching at the same time. Between the two of us we were making less than $2,000 a year. Something like $1,500. So we decided if I took this job and she kept her job we could safely get married. So we ~~got~~ married on Friday the 13th, ~~but~~ before we both went to teach ~~at~~ school in September. I went on up to Rocky Mount and left here in southwest Virginia. The first thing that happened after I went to teaching school as a result of this examination is I was offered about the first of December a temporary job for a month grading Civil Service papers. I declined the job because it was temporary. In January I was offered another temporary job for two months doing some kind of work statistical in nature for the government... ~~I think this was for the~~ War department because

it was a temporary job and didn't suit me. And then about the first week in March I got this this telegram offering me a permanent job as a junior cryptanalyst at $2,000 a year. Headquarters in Washington and to start work on the first of April. Well this excited me because after six or seven months I was disenchanted with teaching high school kids. I was tired of being separated from my bride. She was tired of being separated from her husband, and Washington sounded like Shangrila. So I called her up when I got this telegram and said, "Looka, How would you like to go to Washington, sort of, darling, and she said, "What do we want to go to Washington for?" and I said, "I got offered a job. It's $2,000 a year," and she said, "my goodness, sort of, That's alot of money. What are you going to do?" and I said, "Well I was going to be a cryptanalyst." "What's a cryptanalyst?" and I said, "Honey, I don't know." And so I didn't really know, and after being prompted by her, sort of in her curiosity, I began to wonder maybe what a cryptanalyst was. I said, "Well, look I don't really know what it is," and she said, "Shouldn't you know if this is on the telephone now, shouldn't you know before you get into this." And I said, "We'll get $2,000 a year in Washington, sounds awful good to me. What do you think?" and she said, "Well, I'll leave it up to you." So I decided I'd take the job. I accepted it and came to Washington sort of without, well, in total ignorance of what I was getting into. This was in March 1930 and I reported for duty on All Fool's Day, not knowing what it was. Actually when I looked it up, when I went back to my room I got another little dictionary that all school teachers have and I tried to find cryptanalyst in that dictionary and I didn't. So when I went back to the high school library next morning I looked it

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

up, tried to find the word cryptanalyst in the big, thick ~~Underbridge~~ unabridged dictionary they had in the high school in the library. I found several words ~~like~~ I found "cryptogam" "g-a-m" and that's the study of certain kinds of plants, and of course the basic word crypt... In my Latin background led me to sort of think ~~cryptum and it~~ crypt -- tomb? And there was also a great deal of publicity being given at that time to bring back the World War I ~~bit and~~ dead from the grave yards, cemetaries in Europe and I kind of figured ~~that~~ they were doing some ~~kind~~ sort of statistical work with the crypts and so you, this of couse was foolish, but it was the only clue there was in the whole concept, and I didn't really know what was expected of me as a cryptanalyst until maybe three or four days after I went to work in April 1930. ~~That thing roars like a lion, don't it? Are we o.k. now?~~ I think it's important to understand what ~~kind~~ sort of a climate existed in the military services at ~~the year~~ 1930. The most important element of this is the fact that Secretary of State Stimpson, when he learned of Yardley's activity conducted in New York City, he was considerably disturbed and immediately decided that it ought to be closed down. And I think this has been very well recorded in the context of, "Gentlemen don't read the mail of other gentlemen," so I'll not add anymore to that. But we do find a situation where G-2 was most distressed because they had depended on Yardley's ~~help at~~ outfit as filling this potentia war requirement of a cryptanalytic ~~resourvior~~ reservoir in case they needed to do any studies of communications of other nations if a war broke out; and they were very well satisfied because at that time the priority ~~of~~ lies of interests were Japan (1), Germany (2), and Italy (3)... The three major powers ~~opposing~~ the English speaking world. ~~and~~ There

~~TOP SECRET~~

was a great ~~espere~~ rapport between the English and the Americans and there was no thought of them as an enemy, ~~although~~ although we did have war plans which visualized attack by other nations including England. But Japan was our ~~#1~~ number one target and of course Yardley's work on the Japanese codes for ~~in~~ the Washington Naval conference was exemplory, and this satisfied the G-2 requirement for a Japanese ~~reservior~~ reservoir. There was one gap though that was not provided by Yardley in his activity and that was the construction of codes for U.S. military purposes. G-2 was responsible for the intelligence production, including the kind of work by Yardley in the Black Chamber. The Signal Corps, and this was under the responsibility of the Chief Signal Offic had to provide secure codes and ciphers; had to employ... no, no, I'm sorry, had to provide secure codes and ciphers for use within the Military establishment; had to provide the communications necessary for communications within the military establishment... This was the ~~wire~~ lines ~~orlons~~ and the radio ~~circuits~~ circuits; had to deliver these secure codes and ciphers ~~to~~ to the ~~ADJUTANT~~ General's office who was running the code rooms and storing and distributing the cryptographic material. So you see there were three pockets ~~under~~ into which these activities, generally grouped under the head of cryptology, were administered; and there was very little communication among these. The ~~signal~~ Signal Corps activity responsibility was under the direction of Billy Friedman ~~---~~ an ~~That~~ That's William Frederick Friedman who ~~was~~ very well known -- and he had a secretary and one assistant helping him prepare all the codes and ciphers and invent new methods and improved methods of enciphering for military use.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

The Adjutant General was running the code rooms and storing and issuing the documents. And I'll come back and talk more about that later. (Q. [illegible] Did they do any cryptanalysis at that time?) They did no cryptanalysis in the Adjutant General's office. The only cryptanalysis that was authorized was in the military in the war department establishment was satisfied by the Yardley's ~~right~~ Black Chamber. Friedman's cryptanalytic work was always that which was in support of the code production, and cipher production program. And he was not authorized to work on the messages of other nations, which was Yardley's responsibility. The ~~action in~~ Adjutant General got this because I think it grew out of the Civil War. The Adjutant General ~~would run~~ ran the message centers, you see, and they ~~had~~ just hadn't got around to changing things. And it went through World War I this way. As a matter fact, the code room which used to be run in the old State, War & Navy building that serviced the Secretary of War was run by the Adjutant General, and the Secretary of War used to go down waiting for the messages to be decoded because there was so many urgent messages coming from Paris, The Headquarters of the AEF, that they had to take them in the order in which they were filed or received, and sometime urgent telegrams just didn't get decoded for three or four days. And if you will remember your history, and I know this, ~~this is~~ there's a story told to me by Mr. ~~Benjamin~~ Benjamin F. Smith who was a code clerk in the War Department code room at the end of World War I, He said that the Secretary of War was sitting outside the code room for several hours waiting for them to find the message announcing the armistice. If you remember that came out in the overseas news but ~~there was no~~ there was great silence from

Washington for several hours after the armistice was agreed upon, in World War I. And this was simply because they didn't have enough people decoding messages in the War Department code room to get that particular message out and get it to the president, and the Secretary of War, and the other people who needed to know. I think this is a very dramatic sort of comment on the lack of appreciation for speed and efficiency in terms of fast coding and decoding that has existed throughout all of history up until just about the time that radio communications came into being because that set a whole new pace for the cryptographic requirements. Now, (Q. [illegible] you think this development of the three distinct agencies handling cryptologic functions were simply an outgrowth of traditional developments, and there was no thought given to centralizing cryptology?) That plus the great reluctance and high amount of inertia which all bureaucratic activities suffer from. You never give up something that is important. And you're not sure that you should give up even if it isn't important because you don't know what you're losing And I think it was that. (Let me talk a little bit about the Navy. I don't know as much about the Navy as I do about the Army but I do know that the Navy was not a subscriber to the Black Chamber activities. [It might be important to note that the State Department funded Yardley's activity, in the main, with a contribution of $10,000 a year from the Director of Intelligence, G-2, that was the Director of Military Intelligence, and this was G-2's way of buying into the operation. The Navy made no such contribution and so it was only at the generosity of the State Department that they got any intelligence out of it.] Also there much motivation in those years, in)

(the years 1920 to 1930, in the Navy to become involved in intelligence production from code messages. I think there was ~~it was~~ a glint in their eye but they just hadn't ... they had so many other problems they had to solve that they hadn't gotten around to it, but there was a strong desire, a great motivation within the Navy to update their communications and to have high speed equipment to encipher and decipher messages both on the shore installations and on the major elements of the fleet -- the battleships for example. Now there was little if ~~or~~ no collaboration between the Army and Navy in those days. That developed later.) Another important aspect of the Yardley organizations being broken up by Stimpson was that it galvanized the War Department ~~and to~~ into some action to make a strong thrust at producing intelligence under it's own control. It found out really the hard way that It could not ~~rely~~ rely on anybody ~~in~~ but the War Department for this most ~~battle~~ vital source of information and there were some real forward looking gentlemen involved in this. There was ~~the~~ a Colonel O.S. Albright, who was a signal officer in charge of the communications desk in G-2 who surfaced the problem, ~~and~~ He and the Chief Signal Officer and the Director of Intelligence, G-2, worked out an arrangement, a concept, and a plan whereby they would take the $10,000 that fell out of the Yardley operation and hire a small group of people which would be located in the Signal Office itself, ~~opposite~~ the Office of the Chief Signal Officer, under Friedman's direction.. Friedman was already in being ... and operating under the responsibiliti already ~~described~~ ascribed by the Chief Signal Officer for the production of codes, utilizing the concept that you had to have a full understanding of cryptanalysis ~~that if you were going to~~ produce good codes.

~~TOP SECRET~~

And so they used this device and the money, the ten grand, that fell out of Yardley's outfit to hire some specialists in ... that could be trained in cryptanalysis. At $2,000 a year this provided ~~for~~ four junior cryptanalysts. The remaining funds would provide for a couple clerks and the Chief Signal Officer would make up the slight $800 difference per year, 'cause he already had a couple of clerks and Friedman's salary was already authorized. So now we see the fiscal background for the establishment of the cryptanalytic organization of the Signal Intelligence Service.

Q. (They wanted to make a complete break with Yardley and his people too, didn't they?) [They had no choice because Mr. Stimpson was very strongly inclined to kill Yardley's outfit because of his statement namely that "gentlemen do not read ... etc." And they were also afraid if they put this in G-2, that some inkling would get out that it was being established ... this new outfit was built up for intelligence purposes, and if the Secretary of State found out about it he would say, "Let us not do that even in the War Department;" and the opportunity then to develop the skills necessary for the production of intelligence in war time when it would be very valuable would be lost to the Army ... not because of its own doings but because of the State Department's attitude.] (They also kept this pretty quietly from the Navy because there was really no reason for them to discuss this proposition with the Navy, as I understand it, because the collaboration was not very ... not very good at that time. The word good is not the right one, but it just hadn't developed.) It was pretty much an uncertain field and both sides were proceeding with caution.

Q. (Schorreck) There was only Safford and one or two others anyway. Yes, and most of the discussion was in terms of exchange of ideas

about cryptography rather than cryptanalysis. ~~I'm not~~ might, This might be a good place to mention that Friedman had done a most magnificent job in testing the Navy devices. This is the solution ... Friedman's ~~plastic~~ classic solution of the Heb~~ron~~ern cipher machine. Heb~~ron~~ern was an inventor from California who had developed what he called a coding machine, and we can find this well described in the ~~Patton~~ patent applications, and I'm sure ~~their~~ the in the library because I have seen them there. And the Navy was so intrigued with this device which, ~~in about~~ by today's standards, was terribly slow and inadequate thing, but by standards of 1930 ... (it was a) magnificent step forward in the state of the art because you could automatically encode and decode messages with this device and store ~~a~~ great quantities of keys in a very small package -- which is one of the requirements of a good cryptographic system. You didn't have to have ~~a~~ great sheets of paper and ~~a~~ great big books. You had a little set of wheels and a little ~~of pamphlets~~ pamphlet and than you could reissue the ~~phamplet~~ pamphlet and reissue the wheels and you could have a whole new cryptographic system if you had the facilities for the mechanical production of these wheels. And if you dared use them longer, this was a concept ~~voiced by~~ the Navy, ~~you could learn to use the wheels~~ if you dared to use the wheels for for an indefinite period of time. You could, by rearranging the order of the wheels and the keying instructions for setting the wheels at the given starting point for message, achieve a greater degree of security than you could with a code book and with considerably less expense. Very fortunately for both the Navy and the Army, Friedman took this pioneer~~ed~~ device produced by Heb~~ron~~ern, analy~~s~~zed it, and through a very clever statistical approach was able to force out the answer and establish that an answer could be forced

out of a reasonably small volume of text. Do you remember the date of this? A. This was in sometime between 1925 and 1930. ~~I would~~ I'll tell you this is written up . Well, its before 1930 though. A. Oh, yes. And I'll talk a little more about it later, but the major examples that we worked on was to try to duplicate Friedman's solution of the Hebern machine in our training course. He confronted us with this problem and said, "let's see what you three young men can do about it." Now let me talk about the use of this $10,000. The idea which had been generated by Albright, that's Colonel Albright, and the Chief Signal Officer and Director of Intelligence was that they would get four people with mathematical and scientific training who had studied language in college and get them very young. The younger the better. The difference between these people would be in their major language. I had German. I had six quarters of German. I qualified for a major in college but I knew probably less German than I knew Latin. I'm not basically a language person. Kully -- Dr. Solomo Kullback -- ~~Coleback~~ had studied Spanish in New York. Sinkov, Abraham Sinkov, who was th third of the three cryptanalysts, ~~The~~ junior cryptanalysts, had studied French, and Friedman had no trouble finding three from the junior mathematicians ~~register~~ register, that I described earlier who qualified (in) German, French, and Spanish and but he couldn't find anybody with the Japanese language background, which was the fourth, who had the scientific background desired for his concept ~~for~~ of what you would have to know in order to become a cryptanalyst with the least amount of trouble. The three of us who were ~~then~~ hired then to fill these ~~spots.~~ slots... I came in first, quite by accident, because I was able to get out of my teaching duties ~~much~~ easier than Abe and Kully... That's Dr. Sinkov and Dr. Kullback ~~Coleback~~

So I made the schedule of first of April. Sinkov came in second, he came in shortly after the tenth of April and Kelly came about the ~~20~~ twentieth or the twenty-first. ~~21~~. Now this was a kind of important of thing as we looked into the future because in the military concept your date of rank is a very important thing, and I out ranked Abe and Kelly, ~~and~~ although I must say that's about the only difference. We were all three real neophytes in the business and as developed later we went different directions in our interests. It's important to note, I think, what was done about the fourth. There was a congressman from Virginia... ~~A nice~~ the district ~~from~~ of Virginia which quite coincidently is the district in which I was born in Virginia... Rose Hill, My birth place, is in this district. And the ninth district ~~in~~ embraced Smithville, Virginia. This congressman, Joe Schaffer, had ~~enough~~ a nephew who was not a mathematician and who, in fact, had signed up for more mathematics courses at the University ~~in~~ of Virginia than anyone of the other three of us but never passed a single course. He signed up for college algebra every quarter he was in University of Virginia, but he just couldn't make it. He just wasn't mathematically inclined. Joe Schaffer found out that the War Department was interested in hiring a Japanese expert and his nephew, whose name was John Hurt, needed a job. So he came over to the War Department ... and I remember him talking to Friedman... He came into the office and I saw Joe Schaffer. I had seen him before down in the ninth district. Of course I didn't dare at that time to make myself known to him. I saw Joe Schaffer come in and talk to Friedman and over heard some of the conversation about his nephew, and Friedman was of course not fully aware of I'm sure of Hurt's lack of understanding of things, mathematics. And this

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

is not said in criticism any ~~critism~~ of ~~her~~ Hurt or any derogatory sense... ~~since~~ Johnny Hurt just didn't like math and he just didn't want to be bothered with it, and he ~~just~~ couldn't cope with it. It just wasn't his nature but he was terrific in languages, and it was ~~the~~ that sort of a balance that you'd find in some people, ~~other than~~ evident in Johnny, where his weakness in scientific and mathematical things was more than ~~commensated~~ Compensated for by his ability in ~~liguistics and~~ linguistics. When Friedman was finally persuaded to give Johnny Hurt a test by the pressures ~~that~~ that I am sure that Joe Schaffer brought on him, and that the upper ~~essence~~ echelons of the War Department brought on the Signal Corps to "get's satisfy this congressman because this is the way we make things work with congress..." ~~When Friedman was finally persuaded to get this test set up~~ he got an officer from G-2 who's name was Criswell. Criswell I think is probably better known for his dictionary, English-Japanese Dictionary than he is for anything else he did in his military career because he was a language student in Japan and was really seized with the idea of mastering Japanese. And he put out a military dictionary or a military... I'm sorry... a dictionary which stressed military terms as a part of his language studies in Japan and it was an excellent dictionary. We used it later on. He gave Hurt this examination and I think it would be interesting for me to report what I remember of what Criswell said about Hurt when he reported to Friedman about Hurt's ability. The examination had been given down in the G-2 area. Criswell, after the examination was over, ~~which now~~ and he spent quite a bit in ~~getting~~ giving this examination, came up sort of breathless and ~~stary eyed~~ starry-eyed and said, "Friedman I have never seen a white man who knows as much ~~as~~ Japanese and who is as great-

~~TOP SECRET~~
~~HANDLE AS COMINT CHANNELS ONLY~~

a master of the Japanese language as this fellow Hurt. And You know he's never been to Japan, and where Mr. Hurt had learned his Japanese ~~was~~ first as a child. He had been ~~was~~ interested in French. He was very good in French. He was an excellent French linguist as well as the Japanese. And he had become ~~begun~~ interested in French because his family had owned one of these old ~~little~~ Books of Knowledge, if you know how they have little sections where they put in French phrases with the English translations and Mr. Hurt had become interested in French at about eight or nine years old. And Mrs. Patton a next neighbor, who was the wife of a missionary and who had herself spent some time in Japan and had to come back from Japan because the family had ~~become attracted to~~ contracted tuberculosis, was back in the states and she found young Hurt was interested in Japanese and languages and she started teaching him Japanese and he continued to study under her, ~~and~~ then when he went to school he went out of his way to room with Japanese students and they spoke Japanese ~~continuly~~ continually and he was a great admirer of Lafcadio Hearn who was I think pretty well known in literary circles as somebody who loved Japan and ~~thinks~~ things Japanese, and Hurt was just really good. He was also a very master of the English language and could turn a phrase just about as cleverly as anybody I ever saw. So he was a tremendous translater and, although I can't say much for his interest in mathematics, [~~I think that's important.~~ One of the interesting things about Mr. Hurt's background. (~~I'm~~ I am getting a little tired. Maybe we had better... [Q. move to separate line) Yeah, well cause we're going to go down in about 20-25 minutes, We're going to head down to ~~to~~ the ~~other~~ building.] I think this might be of interest to somebody. I remember that one Monday morning Mr. Hurt didn't come to work until about noon time.]

N.B. Recommend that all bracketed statements be deleted.

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

(tape cut)

He had that they no longer had this ~~resouvlor~~ reservoir of capability to deal with the communications of other countries. They were seized with the requirement to do something constructive about remedying the situation. And this of course led to a concept which integrated all the cryptologic activities. The three units. The Adjutant General, the G-2 activity, and the Signal Office activity into one unit because it seemed to be the most economical and efficient way to Col. Albright and the Chief Signal Officer and the Director of Intelligence to achieve the organization they wanted. ~~Now~~ You remember now that $10,000 is not much money. And in that day it was quite a magnificent ~~sound~~ sum, but it still ~~wasn't~~ wasn't enough to do all that ~~had~~ needed to be done. And also, there was no collaboration between the Army and Navy to speak of, and the fear on the part of the Army that if the idea got around that the G-2 people were usurping the intelligence production by cryptanalysis concept that it would be nipped ~~bing~~ in the bud and they were afraid they couldn't start it again. Now the Chief Signal Officer offered an excellent cover for this activity, and they ~~thought~~ felt they had to bring it all ~~up~~ altogether, for security purposes as well as effectiveness of the organization... so the Adjutant General's functions shortly after the first of April, I think this was about mid-summer 1930, were taken over by the Chief Signal Officer and these functions were: the operation of the code room and the War Department message center. That was ~~about~~ brought from the State War and Navy building down to the Munitions Building; The storage and issue of the codes was taken over by the Chief Signal Officer; And the distribution of the messages which the Adjutent General had been doing as a part of the Adjutant General's function was separated fro

~~HANDLE~~

~~FOR CREDIT~~

Adjutant General and given to the Chief Signal Officer, and at that time sort of probably as a sep to the Adjutant General's office the distribution was made through the Adjutant General by the Chief Signal Officer with the Chief Signal Officer maintaining security control of the messages themselves, because it was realized that if the text of a message, unparaphrased, got out, could destroy the security of the codes. Of course, this was looking forward a little bit because the codes that were in use in 1930 had been in use for sometime and I'm sure were compromised as a matter fact, it came out later, I learned this part of information from the Italians, that the military intelligence code No. 10 had been photographed. The full contents of the military attache in Rome had been photographed by the Italian secret service, the intelligence service... Actually by the carabinieri in Italy and later on had been given to the Germans and finally wound their way up in Finland, via Finland back to Japan. And so there was quite a vulnerability of American codes. [redacted] rooms.

OB40 was not confined to just working on German as we learned from Blinker Halls, Admiral Halls, memoirs and his book on OB40s activities. Now Friedman and Albright and the others who were privy to this operation were aware that extra special security arrangements had to be made for the new codes which were then

EO 3.3b(3)
OGA

[redacted]

Tape 1 Side 2

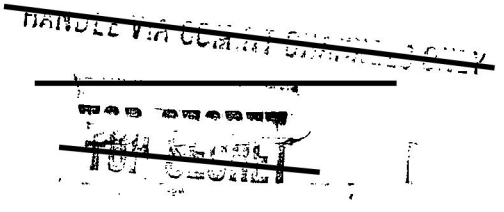
(644) When we went to work we were getting a limited amount of intercept from the Second Signal Service Company up in Ft. Monmouth. This was good copy, and I'll get ahead of my story a little bit because I think this graphically represents a sort of a state of development at that time because it was not until maybe 18 or 24 months after we went to work in April 1930 that we began to get any results from San Francisco and only because an officer familiarly known as Joe ~~Mobern~~ Mauborgne who later became General Joe ~~Mobern~~ Mauborgne, Chief Signal Officer, was out in the 9th Corps area, ~~and~~ He set up in his basement an intercept station controlled by an alarm clock which he had rigged up as an automatic time switch. ~~and~~ He would have this thing kicked off by the alarm clock just when the radio station in San Francisco started to deliver its log to Tokyo because this was was on a pretty rigid schedule because of the propagation ... well, ~~it was~~ there was a time when they could get through to Tokyo and that's when San Francisco went on the air. ~~and~~ He would make a tape recording of this, which was of course in Morse code, and he would air mail these back, these tapes that he had collected, each day's bunch of tapes was sent back to Washington by mail, registered mail I presume, and we'd get them. The reason I remember this so vividly is when we'd start ~~work~~ and work on getting the Japanese effort organized to work on the Japanese codes, the best intercept we had were these tapes which General ~~Mobern~~ Mauborgne, or Colonel ~~Mobern~~ Mauborgne at that time, had collected in his basement, ~~and~~ the way we got the information the intercept off the tape was Dr. Kullback and myself would do the transcription operation.

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

Now these tapes I better describe because we'll think in terms of magnetic tapes. They weren't magnetic tapes. They were the undulator tapes produced by a little pen which drew wiggles on the tape and you could read the dots and dashes by the mountains and valleys which were shown on this tape. I would read the tape and dictate it to Kully who would copy it on the back of a weather report. The Chief Signal Officer was responsible for putting out a daily weather report to the spread it throughout the offices ~~in~~ the Munitions Building, and they'd run off extra copies and it was such a great ~~dealth~~ dearth of paper and the shortage of funds to buy new paper that we would take these old meteorological reports and use the back of them and Kully would transcribe the letters of the message which I would read from the undulator tape and that was our worksheet. I mention this because I think it shows that the intercept service was developing slightly behind but maybe in full step with our capability for dealing with the production of intelligence from intercept. We were really denied access to the cables until it became evident from other evidences, and this was up pretty close to the beginning around 1940, We didn't have any pickups from the cable companies, then we worked up one which I'm sure is discussed in the history. Without this intercept service through there would have been no point in developing the cryptanalytic capability for intelligence production.

Q: Col. Mobern Mauborgne was doing this on his own wasn't he?

A: With official sanction of course, but he was doing it without, with a minimum knowledge of other people and he was doing it



because he was a dedicated man and he was, as well as Col Parker Hitt, ~~Hit~~, they were good friends, knew the importance of getting on with this, this project of cryptology they had conceived and thought ought to be incorporated in the War Department structure and I guess history proved ~~them~~ they were pretty close to right.

...Of how to train us was to set up a series of problems and he had a course in cryptanalysis which he had specially developed for these four candidates, junior cryptanalysts, that had been hired. Technically only three of us were junior cryptanalysts and one was a cryptanalyst aide which was Mr. Hurt because Mr. Hurt didn't qualify because of his lack of mathematical and scientific training for the junior cryptanalyst slot, and anyhow he was on a special slot which was a sort of an exempted position as I recollect. So Mr. Friedman looked on us as a team of four without any regard to the distinction between Hurts official status and ours and it didn't make a bit of difference to us because we were all ignorant you see, we didn't know anything about cryptanalysis. We started off... the first lessons in cryptanalysis I had were in what we called the ~~Levinworth~~ Leavenworth manual, which was a little brown covered publication about five and a half by eight inches, and I have a copy if you don't have a copy... It was a copy Friedman gave me when I was a student and I kept it and its in a leather binding different from the one you ~~have~~ got in the library, if you indeed have one, and at the end of this book after it was quite a few pages, I think I'd say 100-125 pages give or take 50, on techniques there were a set of problems which we were supposed to solve, and then some

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

answers at the back of the book. The books we got had the answers torn out of them which was, I think, Dave Crawford's idea and I think a very good one because it would work well, I can work ~~in~~ an ~~acrostic~~ acrostic or a double acrostic without looking at the answer. I don't know whether in those days I could have resisted ~~[illegible]~~ cribbing a look out of the book ~~[illegible]~~ anyhow we didn't have opportunity to see the answers but we worked out the problems. They were very trivial, about what you'd find in a crossword puzzle magazine, crypto section. A couple of them were a little more sophisticated because they had transposition. I tell you. The thing they compared most favorably with is this American Cryptogram Association's magazine. I haven't seen one for years... but They were simple problems, unsophisticated ciphers but a lot of fun to do. Then after that he divided us up, after we'd gone through this, he divided us up into two teams; Abe and Kully, (that is) Sinkov and Kullback as one team, and Hurt and Rowlett as the other team, ~~and~~ The idea here was healthy competition will stimulate the students, and there was a lot of onerous, clerical work that needs to be done and two people can make twice as much progress as one and this kind of thing and it was a wise idea that he had because it worked out very well. Competition was pretty strong between us because we were "eager beavers" and wanted to show our capabilities in this field, so we worked real hard to outdo each team the other one. There were, oh I'd say, 15 or 20 problems starting out from very simple things, and the last sort of problems were fairly complex ciphers, polyalphabetic

[illegible]

in nature, and in each case there was smaller and smaller amount of text to work with because the less text the more difficult sometimes to achieve a solution. After these problems were finished, Friedman had certain other things that he wanted us to do. For example, the old M94 cipher device which was really invented by Thomas Jefferson and not by (Etienne) Bazeries and not by Parker Hitt and Joe ~~Mobern~~ Manborgne but by Thomas Jefferson before he got to be President of the United States. Do you know this one? I'll write you a paper on it sometime. I think it would make an interesting paper to publish. It would hurt nothing. David Kahn tells all about it in his book, but he doesn't know the whole story. Well anyhow one of the first problems we had was to recover the key, ~~to~~ the alignment of the disc of this old type M94 cipher device, and that was probably the simplest cryptograph that we dealt with. Then we had certain other things. A machine invented by a Swede whose name was ~~Damn~~ "D-A-M-M" which we called the "Damn" Machine because the thing didn't work very well and it seemed a proper name for it, and this machine had a series of interrupter wheels. I believe four which operated in pairs on two, ~~five~~ ten-position commutators. We called them half ~~Hebron~~ Heburn commutators because effectively they did only half of what a ~~Hebron~~ Heburn wheel would do in terms of a cryptographic substitution, and really it was ~~an~~ in effect, ~~of the~~ a combination ~~of~~ of each of the two commutators was a combination of two separate five-letter fractionation squares -- so you got the effect of an interrupter operating on a fractionation

TOP SECRET

alphabet with two different components. This machine was not too sophisticated and we were able to do it without too much trouble, ~~and~~ Then we went on to the Kryha machine which was a rather cranky, clumsy, awkward machine to operate, and it had been invented and developed and manufactured by a firm in Germany, and in effect what it did was to effect a Vigenère encipherment using a mixed alphabet against, starting against another mixed alphabet, and you generate the alphabets by taking little tabs off ~~two semi~~ one semi-circular component which was arrayed along the outside of a wheel that spun and this inner wheel had 52 segments into which you could put a letter so that you got a double mixed alphabet for the other components you see. The reason you had to have a double mixed alphabet was because the first, the outer alphabet was a semi-circular so unless you had repeated the inner alphabet you... well, this is too much detail. But anyhow the Kryha machine, in effect, had a ~~viganere~~ Vigenère with an interrupter wheel. This interrupter wheel was driven by clockwork mechanism with a spring and after enciphering, say 50 or 60 letters, you had to crank it up like an old fashioned Edison phonograph and then you'd poke a button, you see, and read the letter. The Damm Machine was a little more sophisticated in its construction although it was weaker in its cryptographic principles because it had a keyboard and a battery and a bank of ~~life~~ lights so that when you depressed a key you pushed the control wheels forward which in turn engaged the substitution elements and when the contact was cleanly made, a light would flash up and that said if you push

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

the key "E" was enciphered by whatever light lit up and it could be any of the 26 letters so the Damm machine was a little more sophisticated in its mechanical, electrical concept than the Kryha but probably wasn't as good. Both of them were trivial but they were a lot of fun to do and we learned a lot doing them. There was an old fashioned very primitive Hagelin machine. I believe this was a five-wheel machine. It was a fore-runner of the C47, C--(-- anyhow it was a "30" number because as I recollect, and this ought to be checked, Hagelin numbered his machines with the two digits of the year in which he put them into production, so C37 would have been the model that he produced in '37. If you modified it in '39 it would be a C39. Well, we did one of the early models and sort of as a step in getting ready, preparing for training, this group of cryptanalysts, G2 dug up some money out of its... another fund and sent it to the military attaches abroad, particularly to Germany and England and France and the countries that showed some sophistication in the building of devices, and bought up copies of each one of these machines. They got some bargains because you know some of the companies thought well maybe we could sell this to the US government, and if we sort of give them one we might get the contract - - - but if we make the price too high then they won't buy it. So we had a copy of every machine that could be bought overseas. We also had a copy of the codebooks. We had a very good Enigma machine. It was the commerical Enigma. Of course, The German government had ~~unknowns~~ unbeknownst to us at that time been making plans to use the Enigma,

TOP SECRET

and the commercial model was somewhat different from the one we discovered used by the German navy, air force and army during WWII. Well, we went on problem by problem, machine by machine, taking these in the order of difficulty until we got up to the duplication of Friedman's solution of the ~~Hebron~~ Hebern machine which he had done at the request of the Navy. Interesting... one of the most interesting devices we worked on was what was known as the IT&T machine. [After Col Parker ~~Hit~~ Hitt retired from the Army with somewhat of a reputation as being the outstanding Army cryptanalyst, military cryptanalyst, he had been hired by IT&T and they put up about a 100 grand as I recollect for the development of an automatic cipher machine which they hoped to sell to the State Department for encipherment of State Department messages This was to replace the code books which Hit didn't trust. Well there was a Mr. David Salmon who was head of the section in the State Department that dealt with the encoding and decoding and construction of the State Department codes just like the Signal Corps had to eventually become responsible in the army, and Salmon was the counterpart, let's say, of the Signal Intelligence Service in the State Department. Salmon's office was the counterpart of Friedman's office, the Signal Corps, or the Army. Now Friedman and Salmon were pretty good friends and of course Hit knew about Friedman and had been privy to the plans for hiring the four of us, Hurt, Kully, Sinkov and myself and he knew about the Friedman team as he called it, so he was very anxious for the State Department to have this concept tested out by Friedman's team for his own]

TOP SECRET

gratification probably to see if he did have a good cipher machine. Well I can remember that ~~Hit~~ Hitt brought the thing down and showed us how it worked, and this, of course, was done in response to an official request that Salmon had made on the Chief Signal Officer and which had been agreed to by the Chief Signal Officer, but Billy and Salmon had worked this thing out as a way of insuring that the machine was a proper machine for enciphering State Department classified information. I'll make this a short story. It's a sad story for ~~Hit~~ Hitt because after studying the machine for probably less than a day we developed, Abe and Kully and I, I think this was when Hurt was sick, we developed a technique, an attack on it. It used a ten-letter keyword and one of the ~~fields~~ wheels was so designed that the evidence of the cryptographic setting that it applied, ~~through pinwheels~~ in little pinwheels . . . , you could push, well, you could turn the wheel but there were little lugs on the wheels which caused a contact to make or break — according to whether ~~it~~ there was a lug or not, and the contours on one of these wheels, they were fixed, just didn't, wasn't a very good selection, and so the evidence showed through both statistically in the message and spilled over into the adjacent wheel which worked in connection with it. So it was a great ~~connection~~ weakness in the machine and since this was the ninth and tenth position, and since ~~Hit~~ Hitt had stipulated that he was going to use ten-letter keywords, good English words, we sort of said well now look what we'll do is just make the common endings of all the ten-letter words we can find and we did a little card breaking and

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~
~~NO FOREIGN~~

we just sat down and thought of words like "Washington," "Black Horse," you know... All the kinds of things that you would use for making up a ten-letter key. We find out that "t-o-n" "ton" and "i-n-g" "Ing" and "e-d" "ed" and "e-s" "es" and "l-y" "ly" pretty common, so instead of trying all possible combinations for these last two wheels we took "e-n" "EN" which was pretty common and "e-s" "ES" and "e-r" "ER" and we'd try them first, you see, and when we find a pair that fit them then we'd move on and take off the other wheels. Sometimes we got nowhere and we'd try Washington and actually that was the key word for one of the messages and we found "o-n" "ON" fit we immediately tried Washington, and we decoded the message and we had this machine broken in two hours. A little bit of black magic but... Well, I must say that I admired Col Hitt ~~Hit~~ because when he came, well, we read all the messages... I think it was something like ten, and when we finished the tenth message Friedman called Hitt ~~Hit~~ and Salmon. Salmon didn't come down. He was had a bad leg, club foot, I think, and he didn't travel around much, and I think he felt ill at ease in the military establishment, but Hitt ~~Hit~~ came on down in a real hurry and Hit was I don't know whether he was prouder of us for having broken the machine, or whether he was crushed by ~~with~~ the fact that we had broken it, but I have a feeling that Hitt ~~Hit~~ was more pleased to learn that we had the capability for breaking that machine and he was crushed because we had broken it, because

D.S

Hitt was a real, honest patriot. He was a dedicated Signal Corps officer, and one of the highest types that you could find, and I think while it was a crushing thing to him he did feel that he had made a contribution through supporting and helping organize this group of Friedman's that could do something far beyond what he had ever been able to do, that he was real proud of us as a team. I think this ought to be somewhere in the history because there's a lot to be said about the integrity of some of the people that we were associated with in the military services in those days. Well, probably the capping exercise that we went through to work on the classic Friedman solution of the Hebern machine, and then we were about ready to go on our own. Now while all this training -- this work on the training exercises was being done by us, we spent about half of our time doing other chores such as code compilation, we had a whole body of new codes that Friedman had been charged to get out to replace some of the old codes. As a matter of fact, I think it was War Department telegraphic code 1907 was still be used for economy purposes and the printer's overrun of that had been delivered to a book store in Chicago, and he was selling them, you see, as a surplus and this is somewhere in the history and I think its in a copy of the War Department telegraph code 1907 that's over in the central library. If I ever get over there I'll look it up for you, but it was this overrun that was in the public market, would

Now, ~~The~~ I think it was 1907 somewhere in the first decade of this century. Now I think it was a code that was made probably for use in ~~WWII~~ World War II that they were using for restricted communications in the War Department coderoom. I liked to tell a little experience that I had which I think probably has been lost sight of in the other histories. When we took over the coderoom operations from the Adjutant General's office, Benjamin Smith and Mr. Williams and a couple more people whose names I don't remember came ~~down~~ down as the members of the trained staff who were encoding and decoding War Department messages. There wasn't too much code traffic in those days. The security of military communications had deteriorated to the point of where the only distinction that was made between a ~~secret~~ SECRET and ~~confidential~~ a CONFIDENTIAL and ~~restricted~~ RESTRICTED message was the first code group of the message which was the code group for whatever the classification of the message. For example, if the message had been stamped SECRET then the first code group of the message was the code group for the word SECRET which was looked up in the code. CONFIDENTIAL was distinguished from SECRET by

(Hank)

(Good heavens)

this is true and if you look at...

(Hank)

(It ~~did~~ does a lot of good)

Well, you can see why Albright and Friedman and ~~Mobern~~ Mauborgne and the others were distressed, and General Squires was distressed about this because they knew about this and they had no way

of forcing the Adjutant General in the military hierarchy to break off these old practices and use better practices -- and they were scared to death that if they invested all this money in the new codes and a War Department telegraph code is as big as a telephone book and takes lots of hours of careful work to make sure that its properly compiled, the vocabulary is properly chosen; that there are no errors which would introduce ~~garbles~~ garbles into your communication, and if you want a secure code, in those days we thought two-part codes were much better than one-part, and so we wanted to go to two-part codes. We were afraid if we turned these over to the AG without the ~~authorative~~ authoritative control which could be exercised only by people knowledgeable in the technical weaknesses of these things, that all the expense and effort that we'd gone ~~through~~ to would be for no purpose. So that was one of the driving reasons for getting the coderoom under the control of the Chief Signal Officer as well as the distribution and issuance of keys for War Department communications. One of the brightest spots in the coderoom picture was the fact that military intelligence had a special code, it was a 10,000 group code, I believe it was a two-part, I'm not sure at this point, but it was used in conjunction with a set of ten tables which changed every three months. The code groups were five letters, and the tables each consisted of a set of twenty alphabets which would be used in rotation; alphabet one for the first letter of the

code group; alphabet two for the second letter; alphabet five for the last letter; alphabet six for the first letter of the succeeding group and on through the twentieth, the last letter of the fourth group which would be the twentieth letter and then it would be repeated maybe two or three times, then you would insert an indicator which said go to some other table which would be specified by the indicator and then you would apply this new table, so you had a sort of an erratic interruption, ~~in~~ the use of these tables, ~~but in~~ for the superencipherment of the code group. This set of tables and that particular code, or these sets of tables and that particular code were

[redacted]

EO 3.3b(3)
OGA

safe, and this is a wonderful story -- I don't know whether it is true or not but it sure makes good listening if you can tell it well. Now our duties, of course, was to watch these codes being used

to try to come up with recommendations for their improvement and improve ~~codercom~~ code room measures. I'm not so sure this latter was wise because you see we were just young fellows and we had a lot of opportunity to study math in college and a lot of opportunity to study ciphers and codes, both their construction and their solution, in Friedman's courses but we had no practical experience in communications techniques and procedures and code room procedures so it was quite a revelation, particularly to me, when I went back and found out the difference between a ~~the~~ SECRET and a CONFIDENTIAL message was the same code book but a different code word at the front, and I had a little more respect for the MA code. This was MI9 or MI10, and incidentally it was MI10 which almost brought a rupture between the US and UK early in World War II ~~WWII~~ because there was a military attache I think his name was Mead, John Mead, who was sent over as an observer and he took this code along with him, the MI, ~~MI~~, I believe it was the MI10 code and a special set of cipher tables, and he'd attend a briefing and the end of every day, you know, when the British were ~~following~~ fighting Rommel ~~Romal~~, and the next day he would send a message enciphered in this code giving the results of the briefing, that's the war room briefing. It soon became evident to the British that their reading of ~~the~~ Enigma traffic, that there was a daily summary of this war room briefing falling into the hands of the Germans because

~~TOP SECRET~~

there was a German cryptanalytic organization somewhere in Germany which was radioing these summaries to ~~Rommel~~ Rommel's headquarters in North Africa and they began to recognize and identify that this had to be tied in with the briefing when they read the Enigma messages through cryptanalysis at Bletchley Park. So you see here were the Germans producing intelligence by SIGINT, if you will, and the British, in turn, using their SIGINT techniques to identify the intelligence, and then using their investigative techniques to try to determine where the leak was and how to stop it.

Q: (Haun) I recall, wasn't he the military attache in Cairo, wasn't he? sending these reports back here and the Germans picked them off?

A: He was attached as I recollect and I may be wrong on this because I remember briefing him. It was a Major John Mead and he was identified to me as the observer who was being attached to the British forces in North Africa. Now I believe there is what's known as the "~~Fellows~~ Fellers' incident," and I believe ~~Fellows~~ Fellers was the military attache, but John Mead was the observer and probably he was using ~~Fellows~~ Fellers' code room to file his message -- so you'll hear about this either as the ~~Fellows~~ Fellers' incident or the Mead incident and I think there was ... I remember Mead as the observer but I think there were more one, there were two or three observers. I believe ~~Follows~~ Fellers, though, was the Military Attache. This is an obscure point in my

memory so it should be checked.

Q: (Wilson) How long would you say was your training period? Did it ever end really, in a sense, or were you continuing training well into the 30s?

A: Every time, Vince I'm going to answer this, obviously, and I'm going to sound a little snotty, but you never quit being trained as a cryptanalyst because as you learn more about cryptanalysis you are then able to devise better codes, ciphers and better techniques, so as each one is developed, sort of in protection against the techniques of breaking it, you have to go and learn, by developing a new set of techniques, how to cope with this thing, so there it's just like any discipline, scientific that you encounter in college... There's no end to how much math that you can be trained in. The only limit to it is how good you are.

Q: (Hank) But didn't you spend in the very beginning, say from '30 to '33, much more time in terms of training, than in actual production?

A: About half and half. Yes. And then our training sort of evolved from a formal set of problems that Friedman presented to us in the individual research. For example, this Parker ~~Hit~~ Hitt device... Friedman had never seen that before so that, as an assignment, was a bit of a research assignment, if you will, It was sort of like you do post-graduate work... You take something that hasn't been done before and you write a paper

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

on it. So we'd take a cipher machine that hadn't been broken before and we'd figure out how to do it. Now the next time that thing comes along, you modify your techniques and hopefully improve them until you've advanced the art. One of the significant things as part of this training that I left out, and I think should be mentioned, was the work on the ADFGVX cipher. When we started looking through the files that Yardley had left as a result of his Black Chamber being abolished by Stimpson, we found a whole mass of German military messages, field ciphers consisting only of the six letters ADFGVX. This was a fractionated system formed by a square that's six letters as the top and side coordinates, and each letter, of course, each pair of letters that you could choose would represent an individual letter of German plain language which was, of course, the purpose of the square. So you could encipher a text in German with a sort of a diagraphic substitution that resulted from the application of this square. Now after the message was enciphered, it consisted of only the six letters, so what the Germans did, because this would not have been very secure, is to write this in the transposition matrix somewhere from 15 to 25 columns and with the transposition key across the top, write the ADFGVX version of a message in the matrix and then transpose it in accordance with this key written across the top of the matrix, column 1 coming up first, then 2 and so on. To decipher, simple reverse. The interesting thing to me about this ADFGVX is (1) that the

TOP SECRET

classic solution developed in World War I was not a general solution, but dealt only with a special case, repeated beginnings, repeated endings. If they found a repeated beginning of substantial length or a repeated ending they could devise the key for that day, solve the key. If they didn't have this repeated or beginning ending then they had no way of solving the message. Friedman had a vision, I think, that his group would someday be able to come out with a general solution so that any message written in this rather clumsy, but to all intents and purposes at that time, secure system, he thought if we could read any message, then that would be a real step forward. So he sicked us onto this problem, got us to working on it and we

End of Tape 1

ed note: a portion of the end of this tape seems to be missing; ditto for the transcript.

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

in the process of construction and they wanted to protect, for as long as they could, ~~the~~ the information about the cipher machine which had been projected ... which Friedman had been working on, and which was under contract and about to be delivered sometime in 1930. G2 had a very commendable attitude, I think, as I look back, because Albright realized that it would take some time for the Signal Corps to get itself organized to duplicate what Yardley had done. One difficulty became evident early on in the operation of our activity and that was that it would be most difficult to obtain from the cable companies in Washington and New York copies of messages as Yardley and his Black Chamber had been able to do [because we were afraid the word would get back to State Department ~~Dept~~ so this] DoS gave an extra impetus to the War Department ~~Dept~~ to develop an intercept service and arrangements had been made to set up the Second ~~a second~~ Signal Service Company up at Fort Monmouth, New Jersey, administered from Washington by an officer who was attached to the Signals Intelligence Service in the Office of the Chief Signal Officer, and the first intercept station was set up at Fort Monmouth. Then it was planned to have one in San Francisco; one in each of the three departments, that would be Panama, Hawaii (the [Philippines] Sixth department); and one in Fort Sam. Now this one in Fort Sam, I think, is rather amusing because if we look at Fort Sam as a good location for an intercept station under todays concept it's about the worst place you could pick; that's Fort Sam Houston, Texas. But they had lots of space out there at Fort Sam and the Signal Corps had a good installation, so evidently this seemed like a good idea at the time.

insert pp 21a – 21t here [see oral history tape 1 side 2]

Q: What was the name of the new Jap code?

A: There were a variety of names for it. The one I remember now is PAK2 and

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

if we look at the Jap history, the Japanese diplomatic history, the B3 history, we can get the whole series nomenclature as it was lined up ~~in.~~ there. One of the research activities that Friedman got us to undertake comes to mind as probably one of the most important developments that we were involved in in the early days of the Kullback, Sinkov, Rowlett, Friedman efforts. During ~~WWI~~ World War I the Germans had introduced a field cipher. The messages in this cipher could be identified because they contained only six letters of the alphabet - A, D, F, G, V ~~&~~ and X. The reason these letters were selected ~~was~~ is because if you look at the Morse code ~~equipments~~ equivalents they are the least likely to be mistaken one for the other, and the Germans ~~chose~~ therefore six letters because - - used in a fractionation type substitution of a square could be developed with six by six cells, or 36 characters and that gave you the 25 or 26 letters of the alphabet, the ten numbers and a couple of punctuation signs which was a very useful thing for field cipher. The use of the fractionation square was the first step, this performed the substitution, and of course the text, the resulting cryptographic text, and the application of this step resulted in a message twice as long as the original message. I think the Germans thought this was a good trade-off because they had trouble in training their operators and if they could train them to receive the six letters with a minimum of error it really went faster than if they had made a more economical choice with a one to one substitution instead of a one to two. Now the next step was pretty clever. The Germans used a transposition matrix, and as I recall the key was somewhere ~~e~~ between 15 and 25 elements long. The way they applied this was normal transposition, columnar

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

transposition by writing, for example, a mixed sequence of numbers from one to whatever the key might be. If it was 18 long they'd write the numbers 1 to 18 across, ~~18~~ eighteen columns of squared paper, inscribe the ADFGVX ~~text~~ resulting from the first substitution process normally into this matrix and then transcribe it by the numbered column. The first column as the first part of the message, the second column and so on. When this was introduced on the western front in ~~WWI~~ World War I the French had intercepted some of the German messages, and there was a French captain by the name of [redacted] Painvin as I remember his name, it was spelled, P-A-I-N-V-I-N [redacted] and there is a very good picture of him in David Kahn's CODEBREAKERS. So if you want to see what a French cryptanalyst looks like, you can refer to Kahn. The picture is very truthful I believe as contrasted with some of the text in Kahn's book. Now ~~Painlain~~ Painvin had successfully solved certain messages in this system. His technique of solution, though, was a very sort of what I would call a special solution because it required similar beginnings or endings in two messages with the same key and the same substitution square. I won't describe how this is done because similar beginnings and endings are pretty well known in the business, but Friedman had a sort of dream, I believe, or an inspiration because he felt that there could be a solution, a general solution, so that every day's traffic could be read. The French solution just gave traffic -- readable traffic only when you found the special case messages, and this was not very satisfactory and you had to wait in those cases until the two messages had been intercepted. Friedman thought it could be done with maybe eight or ten messages long enough, of course, to give certain

TOP SECRET

information that you needed. So as soon as he thought we were ready in our analysis of ciphers and this was I'd say about a year after, -- probably the summer of 1931, he got us to work on the great ~~massive~~ mass of traffic that had been inherited from Yardley's Black Chamber. Well -- I'm not sure whether Yardley had it or whether G2 had saved it but it was in the vault, Room 2742 Munitions Bldg., where the archives of the Black Chamber had been stored after Yardley's group had been disbanded. Well we dug out those files and there was enough stuff for us to work on, but Friedman made up as I recollect, had us make up some test messages in English which were kind of favorable for the kind of attack that he'd hoped for us to use, ~~and~~ so we pursued our investigations and I think in a very short time, maybe a couple of weeks we had developed the outline of a general solution, ~~and~~ then we went down to the real traffic, ~~a lot of~~ live traffic, intercepted during ~~WWI~~ World War I, several... 10-15 years before, and tried out the techniques on that, and lo and behold these messages broke, and then we had a general solution and this general solution is written up as one of the technical papers that Signal Intelligence Service (produced), I think the title of it is "The General Solution of the ADFGVX System." Now this is important to me because the general solution which was developed to solve this old ~~WWI~~ World War I traffic was ready-made for one of the Japanese diplomatic systems that was introduced shortly after the PURPLE solution had been ~~obtained~~ attained, and when the Japs were generally improving their diplomatic communications ~~and~~ the system they introduced was a digraphic, ~~tetographic~~ tetragraphic code, the typical Jap two-letter/four-letter code, and the Japanese text was

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

first enciphered by this two-letter/four-letter set of tables. The resulting text was then written into a matrix a great deal like the Germans did. The only difference between the Japanese matrix and that used in the ADFGVX system is that at the top of certain of the columns the Japs had blocked out, evidently they had a printed form for each one of the transposition keys with a key printed on top, then, I'm sorry, I'm not sure they had the key printed on the top but they had these blocks pre-printed so that the Japs could, if they desired, write in the transposition key at the head of it. ~~The~~ let's say the longest key I'm sure that the Japs used was about 25 and if their key let's say could have been 17 or 18 they would simply scrub off the last columns limiting the key to 17 or 18 and then when they transcribe the message they would operate just like the ADFGVX column by column according to the number at the top of the column and when one of these blocked out cells appeared they simply missed the letter you see. So then we were confronted with a text which was first enciphered by the two letter/four letter charts and then subsequently transposed according to this interrupted matrix transposition key ~~up there,~~ Now this didn't bother us when we started working on the interruptions didn't bother us when we started working on the messages because the message was long enough we simply ignored ... we'd say well it's 25-letter key, we'll divide the long total number of messages by 25, we'll ignore we'll find how long the average column is, we will ignore the first five letters of that column, break it up

roughly into these columns and then certainly the first and last will be a pure "we will know" we won't have to worry about the interrupters in the first few letters that we selected and the last few letters. Now this may get smeared in the message because if its 18 instead of 25 there will be a little bit of accommodation that will have to be made and figured out as we proceed inside the message. Well now the way this system came into effect is we found a whole brand new set of messages that just had new indicators and just didn't seem to work at all. When we tried the techniques of the existing transposition, which was a fairly simple thing, this transposition seemed to be quite different, when it appeared in traffic. Then lo and behold the Navy came along with a package of material that they had procured through a "second-story" operation, Naval Intelligence. I'm not sure just where this package came from, I suspect it was from Chicago or New York because they had worked out a pretty good deal to enter the Japanese Embassy or ~~Legations~~ Legations and certainly in New York, ~~and~~ If I can interrupt here, when

EO 3.3b(1)
OGA

[redacted]

To go back to this the Navy came over with a package, we looked at it with great interest and curiosity, of course, and we discussed it and I

~~HANDLE VIA COMINT~~ [redacted]

[redacted]

remember one of the things Friedman said when he saw this and we were trying to figure out just how we would approach these messages. He said this is more difficult than the Purple machine and I doubt if we will read it. This was his first reaction. Now I mention this because Friedman's words were turned against him because this project of research that he'd lead us into in the ADFGVX came right back to haunt him because it was that trick that he'd encouraged us to develop that enabled us to read the new system. We had a lot of fun with Billy Friedman about his prognostication saying that he'd just forgotten his early cryptanalytic impulses. Needless to say we were all delighted that the work had been done. Now I'm going to continue because this leads us into something that I think is probably the most important thing that I saw happen in the whole field of cryptanalysis -- because in our work on this transposed Japanese code with the patterned after the ADFGVX as I described, we found that the Japanese key changes, four times a day as I recall, plus the proliferation of keys, each area of the world, in some cases, had a different set of keys, so if you had several areas -- and lets say three or four areas times four changes a day that gave you three or four times four, twelve or sixteen different keys you had to recover to read each days traffic completely and we'd long before set the standard that we would read every Japanese message that wasn't too garbled, every Japanese diplomatic message that wasn't too garbled. If we had one laying around and we couldn't read it we worked until we found out why we couldn't read it. So we wanted 100 percent solution to continue and we were somewhat distressed when we found out that there just wasn't enough of

TOP SECRET

us to recover these keys because it pretty onerous task to do by hand. We were using IBM machines, in some sort of a stupid way to help us, but this turned usually to be more work than a clever cryptanalyst would have to expend if he just sat down and forced the text out. Well, Bob Stex Ferner, Furner, Al Small, and Sammy Snyder and myself got kind of worried about this. We were just like the frog; we'd jump up six inches today and fall back twelve inches tomorrow you see. We weren't getting to the top of the well at all and so we just quit jumping and sat down and said, "What can we do to speed up this solution?" and we, it became quite evident that the only thing we could do was to find a much better way of using the IBM machines ~~then~~ than we'd up to that point in time developed. So we did I think the first serious thinking about mechanising a cryptanalytic process. One of the most significant things that came up in that connection was an idea by Albert Small Stet Small Stet early on in his training as a cryptanalyst and he came in several years after Abe + Kully and I did, Small Stet had introduced the idea of substituting for the observed frequency if you were doing the computation that ~~fi square kind~~ chi square type of computation substituting the logarithm of the frequency for the frequency itself and then all you had to do was add the logarithms which was a lot simpler thing than multiply the Mag frequencies. Squaring the frequencies you just double the log sort of -- and if you ~~wanted~~ wanted to match a couple of alphabets you cross added the logs for each one of the letters instead of multiplying. We didn't have these little electronic desk calculators in those days. I wish I'd have had one, I'd been a lot more able as a cryptanalyst. Well that

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

one thing Small did, and he got the better idea which I think is terrific, and which rounded the first concept of using the log of working out a sort of a technique for reducing these logarithms to a single digit so you laid them out on a scale of ten rather than a hundred or thousand as you would if you used a two-place or three-place table. Well now this opened the door to the use of the IBM machine in a very unique way. We could then use the IBM machines to use these logs. IBM machines could add very well but they couldn't multiply efficiently so by simply adding the logs we got an index directed from the machine that would have been denied us if we tried to multiply. I elaborate this concept because it was the key to the next step we took. And the next step we took was to organize a program which could be adapted to the existing IBM machines just as we developed a program today for a computer except we didn't think in terms of a program and the IBM as a computer. We thought of it as a technique which we could employ the machines to apply for us. To shorten this story we built the first Geewhizer. This required a special attachment to the IBM machines and, with our experience with second switches and telephone relays that we'd developed out of the Purple machine attack, it was a very simple matter for us to develop a sort of comutator device that would be hooked on to the IBM tabulator and in this concept of course, there was no memory of any type in the IBM tabulator, but we designed a card and I think Small and Furner did most of the work on this we designed a card that in effect contained the data, statistical data associated with each of the 26 letters of the alphabet as it joined with each of the other 26 letters, and if you will imagine the first

~~the first~~ 52 columns of a card, 26 for the initials, and 26 for the finals, and then the statistics for each column, for each letter, would be written in the appropriate column in, let me say this precisely. The first 26 columns of the card would have the statistics for each of the 26 letters of the alphabet, A in column 1, B in column 2, Z in column 26. Now A, with A as an initial, would be punched in the first column. If it was a four, the logarythmic frequency of AA as it appeared in our statistical charts then would be punched as a four in that column, AB would be punched whatever one-digit logarythm came out to be, say a 9 and that would have been a real high one, and AC would have been a 0 and AD ~~would have been~~ a 1 and so on until you had written in the data for A with each of the other letters. Now that would be as a final. Columns 27 ~~through~~ to 52, the same data except A in the other position; A initial for the first 26 and A final for the last 26 and then you would have a card for B and a card for C and so on. Now these bands, and I've gone at some length, maybe in a useless ~~aggression~~ digression here of trying to describe the cards, but I've tried to lay the groundwork for the concept that the two fields of each card was in fact a memory, and it remembered for us the statistical logarythm equivalent of the combination of these letters each with the other. Now instead of having a drum or tape as we normally think of a memory, the memory was the field of these cards, and that was how we got over the hump of a memory in this "Geewhizzer." ~~Geewhizer.~~ Now another thing this "Geewhizzer" ~~Geewhizer~~ had to do was what we call "Drag" and I'm not going to go into that because it is a little too technical for this type of discussion, but if you want to

look into this ~~Ceewhizer~~ "Geewhizzer" thing you might read a write-up. I think there is a very excellent one somewhere in the histories. Now this lashup, this ~~rigmarole~~ rigamarole of wires, haywire if you will or whatever you want to call it, was the most startling, the most effective tool that I ~~have~~ had seen in the years that ~~I have~~ I'd been working, including all the work on the Purple, the work on the ECM and all the other machines. This was the peak of cryptanalytic achievement even though it looked like something that come out of a ~~Rup~~ Rube Goldberg ~~column~~ cartoon. Now we started using this, of course, we didn't have the relay banks, again my Thomas Edison impulses, I wound up by wiring up these banks, ~~and~~ of course we kept the IBM service man out of the room because it was classified. There was a rule IBM made. You couldn't hook anything onto the machines but we ignored this. We went in and changed the wiring and when we had trouble with ~~the~~ our tabulator we actually had to go back and put the wires back before we could let the man test the machine. This was a kind of routine we went through until we finally got him into our confidence. He was a good guy. Well after, oh I'd say about six weeks work, and it went pretty fast once we got the program laid out, we began to turn out keys that produced much faster than with the hand methods and most gratifying to us we were able to solve messages that we had not been able to solve by our hand techniques because we could change the tables very rapidly, you see, by simply punching up the new deck of cards. And that was the memory. We could change the memory just through the routine. Maybe take three or four hours which was a long time which would be a long time by today's standards but by our

[redacted]

[redacted]

standards it was a lot shorter than ~~by~~ doing it by hand. Now, ~~The~~ of course, throughout this approach on the new transposed Japanese code we collaborated very closely with the Navy, ~~and~~ we exchanged technical ideas and we kept them aware of what we were doing with this ~~Geewhizer~~ "Geewhizzer." I think they didn't have much faith in it, as I look back, because ~~they were~~ they knew the hand methods would work, and so they didn't have quite the impulse to deal with IBM machines and utilize them that we had in the Army and so they maybe didn't have the faith we had. Well pretty soon, they began to be amazed at how many keys we were pulling out, and we were pulling out keys that they couldn't pull out, ~~and~~ so there was an Ensign Hargraves that was very much interested in this. This was his job... to solve the Japanese transposed code. So he came over and worked with us for a few days and he was so enchanted with this device that he said we got to have some in the Navy, ~~and~~ so they ~~me~~... I don't know whether they built theirs or we produced one and gave to them, but anyhow we had a whole bunch of ~~Geewhizers~~ "Geewhizzers" hooked onto the IBM reproducers, that was pulling out Japanese transposed keys for us. I'd like to emphasize this for my own viewpoint as being the most significant step taken in the pre-~~WWII~~ World War II cryptanalytic endeavor in both the Army and Navy and it was far in advance of anything that was done in GCHQ except probably the Bombes that had been developed for work on the Enigma and of course comparing the ~~Geewhizer~~ "Geewhizzer" to the Bombe is a little bit of an apple and orange comparison because the concept of the Bombe was to duplicate the machine, the German machine, and to run it real fast if I can oversimplify the Bombe concept. The concept of the ~~Geewhizer~~ "Geewhizzer" was distinctly different from the Bombe concept in that we were

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

using the Geewhizer not to duplicate the Japanese transposition and try it out to sort of see which one looked the best but we were going in and boring from within using the statistics from what I mentioned earlier, the front first column and the last column of the message. As we drug these letter by letter through the message until we found the place where the last ten letters of the 11th to the 15th ... 20th letter of the first column. The last ten letters of the message are the letters numbered 11 to 20 whatever, 21?, 11-20. We could take letters 11 - 20 and put it in all positions and would be one very good match, Hopefully the pair of columns that joined each other were adjacent in the transposition matrix. The Geewhizer story tells the technical details. I remember them. I think I could duplicate them but I can't describe them well enough for this kind of presentation.

Q: What kind of messages were these used for? Were these diplomatic?

A: Japanese diplomatic messages. Let me talk about that. What the Japanese did in their diplomatic network they had a series of keys for the US. I believe another series of keys for South America and one for Europe and one for Far East. There was some division like this but its been so many years how they divided it up is a little bit elusive. Now this transposition system equated in its importance to the Purple and was used in those Japanese installations, diplomatic installations, not military, where they had no Purple. As I recollect the Purple distribution was limited to Tokyo of course, Washington, London, Paris, Rome, Berlin, Moscow, Warsaw, Ankara. There should have been ten and I think I mentioned ten cities. Now if the Japanese wanted to communicate with Mexico City which had no Purple machine

and to send a message ~~at~~ of the highest classification to Mexico City they would use this transposed code. If they had a message to send to Washington of similar classification they wouldn't use the transposed code; but they would use the machine cipher. Now if the message was a book message sort of and included both Mexico City which didn't have a machine and Washington which had the machine then it would go in the commonly held system, namely the transposed code because both Washington, which held the code -- the transposed code, and Mexico could read it.

Q: (Mrs.) Did they ever use both to your knowledge?

A: Yes. If a resend of a message was required, for example if a message came to Washington and at some time later they needed to send this message to Mexico City, the message had already been sent ~~enciphered~~ in cipher to Washington with the machine. Now, say three weeks later after the message had gone over the air, they needed to send the text to Mexico all they could do would be to reencipher the message in the transposed code and send it to Mexico City. We had not too many cases but I remember one that was a lot of fun. When we were studying a new, well after we had solved the Purple, we had a case of where there was a normal change of the Japanese diplomatic code which was a forerunner of this transposed code system. This was several years before this new code had come in ... several months before the new code had come into effect, I think it was pretty close, maybe within a year. Our problem was to recover the two-letter and the four-letter charts. When the new code came into effect, I remember Louise Prather, who was in charge of the registration of the Japanese messages, came in to where Turner and Small met and I were working and gave us the text of a message

TOP SECRET

and the Japs always enciphered the number of the message in little auxillary ciphers which didn't change and if it did we could read it in a hurry. The message number on this transposed code text was the same as there one in the machine to Washington, and there was another case where was a resend in this new code of a message in a previously solved code. As I recollect the machine message was fairly short. But the retransmission of the code message was fairly long so we had a duplicate in the old code, the new code, and a duplicate where we had the literal text in Japanese, Romaji, with the new code. Now we weren't that good in Japanese that we could solve a Japanese code. We usually relied on Johnny Hurt and his group, Phil Cate and others to do this. Well Cate Kate didn't like to recover Japanese codes. He could translate. He was a wonderful translator, very capable in language but he just wasn't a good code recoverer. Harold Dowd Doud who was probably one of the best, he and Merrit Booth, Col Booth, were the best that we had working directly with us. Joe Sher Sherr was very good, but Sher came in at a time when there was very little code recovery to be done, but Booth and Dowd Doud were both excellent at code recovery. Well, Dowd had been working on the first few messages that we had produced trying to recover the code, the two-and four-letter charts and, of course, you recovered the two-letter chart first because its got the more frequent ones frequence and then as the four-letter groups appeared, with the less frequent groups they came later. Well, Dowd Doud had been working on this thing on a Wednesday morning. Wednesday afternoon was when the officers were required to take a half day off for exercise, so he closed up at noon, folded his books, put them on top of his desk and said good-bye to us.

start new disk

Prather brought in these messages shortly after he left and we couldn't keep our hands off of them so we did the obvious. We took the text. We took Dowd's worksheets and his partially recovered codes and we made a new copy of them and we added every one of these recoveries which came out solid because the two- and four-letters were just simple, new additions, so they came out just exactly, and we'd recovered enough to read about a third, statistical third of the groups and all the messages received. We did this by the close of business, straightforward trick. So very straight face, next morning when Dowd came in, in with Furner and Small and Sammy Snyder and myself in the room, we said, "Well we thought it was a slow day yesterday, and we thought we'd do a little work on code recovery. You want to check these out and see how bad a job we did." "Yea," he says, "well I'll see." So he goes on in, and I peeked into his office, he had a little alcove in the corner of the building... I peeked into his office and he was doing something, I think he had some correspondence in his, he had to make some kind of report that he had taken exercise the day before. After about a half an hour it became evident that he was going to work on these, we sort of kept him under surveillance, and he looked at it and he got the strangest look on his face, he was real pained and he beating the side of his head, this was a habit of his, and after about 20 minutes of this, he came out and said "What did you all do? I never saw anything AMAZING. He said, 'I couldn't have done this in three weeks.' How did you get all these Values?" Well, it was too good to take it any further so we told him but he was a very distressed man because he couldn't understand the short time we left him in the dark, how we had been so successful. He thought we were real magicians and we had figured out some kind of

device like the ~~Geewhizer~~ "Geewhizzer" to recover the codes for him. And this was the impression he had that we had done this by some super magic that he didn't know about. I'm sorry to introduce this but it was so much fun I couldn't leave it out. As a sort of interesting sidelight on the development of the ~~Geewhizer~~ "Geewhizzer" and I'd like to identify it right here in my own mind, being the first constructive, creative effort at the production of a device which in the form of a computer, primitive as it was, demonstrated that a computer could be effectively used to advantage. The other devices, computer-like things, like the old Bush machine which the Navy developed and some of the other things that had been produced under contract by Eastman Kodak were well motivated efforts into this field, but the were so simple and ~~confirmed~~ confined to such a limited domain of cryptanalysis it was easier to do them by hand or by modified IBM technique then it was to build a special machine. As a matter of fact we discarded all these special devices that had been built very early on in our examination of them because it was more work to use them than they were worth. Now the ~~Geewhizer~~ "Geewhizzer" was quite a different animal because the ~~Geewhizer~~ "Geewhizzer" not only carried its own weight but pushed the frontiers of our achievement. Our ability to read more messages, messages with less information in them, I'm talking not of intelligence information, but less statistical information -- that was so low that our hand methods wouldn't discover it. So it really pushed the frontiers of cryptanalysis far enough ahead so that we proved that a computer could be beneficially and profitably used in cryptanalysis and could do things which the human could not do. Of

TOP SECRET

course you can postulate this latter by saying well if a computer can multiply ten times faster than a human than it will do ten times as much work. The ~~Geewhizer~~ "Geewhizzer" not only took this sort of simple, nonsensical argument that I just voiced, but it proved it by actually setting down and doing the thing itself. So this I think was a breakthrough, probably the most significant breakthrough in cryptanalysis that... well I'm convinced that its the greatest step that I saw in my whole career, and that includes the present day achievements because some of them are real startling but the difference between where we were before the ~~Geewhizer~~ "Geewhizzer" and where we were after the ~~Geewhizer~~ "Geewhizzer" was a greater gap then the difference where we were before some of these newer innovations and where we were after, and that's the way I'm trying to measure it. Now as a little bit of a humorous side light to this thing there has always been the question - which came first, the chicken or the egg? I've translated this into a concept - which came first, the hardware or the software in the computer business? I think historically, if you believe what I've told you, what we did was to develop a ~~the~~ program and then we built the hardware, so the program came first, the software came first, and then the hardware came afterwards. Without the program we would have had no idea what kind of hardware, obviously, we would have to build. Now in a more serious vein, what did we learn about how GCHQ, who was confronted with this system, dealt with it, and what did we learn about the Dutch and how they dealt with it? Of course the GCHQ didn't have a ~~Geewhizer~~ "Geewhizzer" and they were kind of busy with other things like the Enigma so they didn't really hammer as hard on this transposed code system as we did.

TOP SECRET

TOP SECRET

They did achieve a certain amount of success by hand techniques. Now about the Dutch to go up into time to the point of where the Dutch East Indies fell under the Japs. This was, of course, after Pearl Harbor. And the way I learned about how the Dutch solved this Japanese transposed code came about as a result of the assignment of one Col Verkuyl, a Dutch cryptanalyst, who was the head of the Dutch cryptanalytic organization in BANDUNG in the East Indies, and he'd been snatched out of the East Indies, flown as the Japs were coming in, flown to Australia and then shuttled rapidly to Washington because he was considered by the Dutch as their most valuable codebreaker, and they wanted the Americans to take advantage of his abilities, and of course G2, always this syndrome of, 'We don't understand this Army Security Agency outfit. Maybe there are things around the world that they don't know about. They're pretty good but they might learn something." G2 wanted him assigned to the Japanese section, and this was a very strange thing because we didn't much like to let Americans in let alone foreigners, but when G2 ordered us to take this fellow in and put him to work on the Japanese code solutions we had no choice. I remember one morning in March after Pearl Harbor, and at that time I was a first lieutenant, that this Dutch Colonel, I was introduced to him. He was a miserable looking individual at that point in time because it was snowing outside and he had on a summer uniform and he was dead tired and extremely distressed because he made this long trip from BANDUNG to Australia to America within -- just as fast as they could get him there. But most of all he didn't know what had happened to his wife and family who had been left. He'd been ordered out of there, you see, to leave them and he was extremely distressed, emotionally distressed, because he didn't know what was

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

happening to them. Well this happened before lunch and he was brought right in into my office. This was behind closed doors, a sealed off area that we had, and I was told to put him to work. Well I looked at him and I felt so sorry for him, ~~and~~ he was ready to go to work right then. I said, "Do you have a place to stay?" and he said, "No." I wasn't really ready for him so there was a little bit of self-serving in this so I said, "Why don't you take the rest of the day? We'll send you up to the Dutch Embassy, ~~and you~~ find a place to stay ~~and you~~ get yourself some warm clothes, ~~and you~~ do whatever you need to do and when you feel like it you come back here and we will start work but you get rested and get ready to do something because you'll be sick if you don't sort of." He did and we got ready for him, ~~and~~ In due course he became a member of the section. What I did was put him in a room by himself and gave him some Japanese messages after talking to him about it and he said, "Yes, we can read this one." He identified the messages. His ~~e~~nglish was not too good at that point in time because he was out of practice, so there was a bit of difficulty in talking about technical things. Sometimes we'd invent a technical word like a ~~Geewhizer~~ "Geewhizzer" that meant a whole lot to us but was nonsense to anybody who didn't know about a ~~Geewhizer.~~ "Geewhizzer." I didn't tell him about the ~~Geewhizer.~~ "Geewhizzer." My intention was to find out what he could do before I told him about what we could do. Well, he wasn't... his techniques were a great deal like the French solution to the ADFGVX. Again employing the ~~forming~~ similarity to the systems. But they had a special case -- similar beginnings or endings it worked just like in the ADFGVX but these were rare and they'd gotten a break into the system through this technique, ~~and~~ With their knowledge of previous systems they'd done a

[redacted]

[redacted]

commendable job learning the mysteries of this new system. They had read several days traffic by combination of techniques. I think they'd found the repeated messages useful too because there were a few cases of that, ~~and~~ having discovered this much information about the Dutch techniques, and finding the man right in our midst, and also being under pressure from G2 to employ him because he was highly touted by the Dutch officials here in Washington, we finally introduced him to the ~~Geewhizer~~ but we limited his access just to the diplomatic section. We did not give him access to the Purple at that time. Now to get a little away from the technical aspects of ~~Brikile's~~ assignment, his working partner was a young fellow who was fairly good at working on this particular Japanese system. ~~A~~ young fellow, the American's name was Joe Peterson, and this is when Peterson and ~~Brikile~~ became acquainted. The association between Peterson and ~~Brikile~~ I think is very important because Peterson was actually recruited by ~~Brikile~~ to operate as a penetration of the US COMINT organization to the advantage of the Dutch intelligence services. The ~~Brikile~~-Peterson story is well documented and reference to the USIB deliberations and the reports prepared for USIB will demonstrate the importance of the introduction of ~~Brikile~~ into the ASA cryptanalytic organization, and I think should be considered as a case in ~~part~~ point of the need to exercise the utmost caution in our relations with foreign intelligence services. To put it bluntly, the mission of a foreign intelligence service is to produce intelligence without any restrictions on the techniques used. There may be honor among thieves but there is something less than honor between intelligence services. End of ~~morale~~ moralizing.

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

In the COMSEC area of our efforts, in the early days of the Signal Security Service, we had as part of the mission of the Chief Signal Officer the responsibility for improving the cryptographic security and of course the systems that were employed by the military services. Now this ranged from the field ciphers, where the M94 was used, and that was the authorized device, at that time, right on up to the highest echelons of the War Department network. The old ciphers were pretty weak. The codes used had been in effect for years. There was very little concept on the part of the Adjutant General's office of what constituted proper cryptographic security in the sense that they could very well understand locking books up in safes, but they didn't understand the damage of let's say sending too many messages in a given system. The things that a cryptanalyst would employ to break the system ~~would~~ were not understood by the people who were administering the code rooms and the code room practices in the War Department message centers in those days. Now Friedman had made a pretty good analysis of the situation and had concluded quite rightly that mechanization, the use of machines, was absolutely necessary if a substantial improvement was to be achieved. However in recognition of the fact that machines were a new thing and that there might have to be several generations of the machine before we would find one that would be totally satisfactory, he continued the use of planned to continue the use of code books, So as a part of the program which he'd undertaken himself there were new ~~additions~~ editions of codes; a War Department secret code, which was a very voluminous thing. It had something like 50,000 groups in it as I recollect; A War Department confidential code; and new editions of the military intelligence code, we were up to MI, military

TOP SECRET

intelligence code 10 at that time so we needed 11, 12 and so on, and he had started to prepare the manuscripts for the vocabularies of these new codes. Now our contribution, our useful contribution ~~for~~ to this program in our early days of being students was to ~~mainly in was to~~ work mainly in the editorial phase of the code compilation program. This meant, among other things, the preparation of code vocabularies. It meant the preparation of reliable code group vocabularies in the sense that you had to avoid garbles and ambiguities and I'll simply refer to this as the development, or devising of, or the construction of the most efficient permutation tables which could be used for generating the code groups forming the vocabulary; and, of course, cross referencing, cross checking the galley proofs of the manuscripts when they were typed up before they went to the Government Printing Office; and then cross checking the galley proofs after they came back; and then cross checking the final galley to make sure that no single error ~~no single error~~ a 100,000%, if you will, accuracy had been achieved in relating the code groups and plaintext elements of the encoding section with the code groups and plaintext elements of the decoding section. Now this was pretty important, this latter, because sometimes the printer not quite realizing what he was doing would take a slug out of would take a in making a correction, would let the code vocabulary slide one or two places with reference to the plaintext vocabulary in either the encoding or decoding section and every group that was affected by that slide would then become an error. This is only one example of the kind of things we had to avoid. I think from my own standpoint that the drudgery which we had to go through to prepare these codes since they were all done by hand ~~and~~ on 3x5 cards that required typing with a

TOP SECRET

TOP SECRET

Tape 2, Side ~~1~~ 2

Well this all had to be avoided and I think this drudgery which we were confronted ~~with~~ convinced me that Friedman was absolutely right. We had to have cipher machines. ~~and of course~~ There was no argument, of course, as far as I could tell from Abe and Kully who were at that time ~~we were~~ pretty well indoctrinated in what needed to be done to improve the US systems. ~~So There was no question then we had to have machines.~~ Just about this time the machines, which Friedman had developed ~~from the~~ results of his studies and ~~his~~ research into the Hebern device that the Navy had asked him to look into, ~~study~~ was about to come off the assembly line. We had about ~~a dozen items~~ a dozen of these machines which had been constructed by a firm up in New Jersey, Wallace and Ternan, with which the Signal Corps Labs had let a contract. ~~with them and~~ These machines were just coming off the line and we got the first two to test out. They looked pretty good, ~~that is~~ as we compared them with the Enigma, the Kryha, the so-called Damn machine, ~~this is~~ the electrical ~~Hagelin that type~~ Hagelin-type machine that was developed by Damm in Sweden, and they looked much better than the Hebern machine which was a pretty well constructed machine. ~~and also~~ They also looked better than the Mark II for which the Navy ~~had let on had~~ contracted on the second contract with Hebern. They used an electromatic typewriter ~~The one~~ that was built by IBM.

TOP SECRET

~~which~~ It was a very good typewriter considering the state of the art in those days and had a specially built keyboard which Ternan had fabricated in ~~his~~ its own laboratories. The wheels were driven by solenoids and they were controlled in their motion by a teletype tape. [* Now the way the tape controlled the wheels. ~~The~~ Was that it? The tape was punched up with a bunch of nonsense characters and the tape could be several hundred characters long like the key tape in the ~~Vernun~~ Vernam machine which ~~was~~ is described in the patents... That's the old two-tape system that Friedman incidentally broke and which was one of the earlier exercises that he gave us in our training as junior cryptanalysts. So the key tape principle was taken from the ~~Vernun~~ Vernam concept and applied to the wheel stepping concept of the ~~Hebron~~ Hebern machine to produce an unpredictable motor key -- hopefully to keep the wheels in motion for the encipherment of any message.] Now, ~~the~~ these machines had not been field tested, so after testing the first two delivered by the manufacturer, approval would be given to go ahead with the remaining machines. ~~and~~ When they were ~~to be~~ delivered they would be distributed to the War Department code center and the three departments and, ~~that would accommodate that had to be sent out in pairs~~ since they had to be sent out in pairs, that would accommodate eight ~~and that would leave~~ and a couple of spares in case things went bad at one of the points where the machines were issued and they had to ~~be~~ replace it. ~~so~~ We also looked forward to having these machines ~~in the office~~ in our working area so we could examine them and

* FBR, in the ensuing lines does not complete his explanation of how the tape controlled the wheels. She thought to leave hanging - I would delete all between: - "Now the way the tape controlled the wheels.." and the sentence that ends: "in motion for the encipherment of any message."

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~
~~COMINT~~

understand them and maybe make some tests on them and do some research ~~and see if we couldn't figure out some effective countermeasure you see which would well we want~~ to prove that the cryptographic principle was good. ~~and We didn't care whether it was~~ we just wanted to make sure it was good. ~~and~~ If we broke it we would have been proud and we would have figured out a better one to incorporate in the next generation of machines. Now at that time ~~our~~ this would be about ~~2 1/2~~ two and a half years after the first of April 1930, ~~We used~~ that as a base time, ~~and~~ the machines which we received ~~from the~~ for testing I would say came in about three years about 1933. This can be verified by looking into the history of the SIGABA. The dates can be accurately determined if they are important. Now as a part of the program, Friedman thought it would be well to have the key tapes which would be issued with each of these machines. Actually the system consisted of the chassis, the machine itself, an assembly of wheels, I believe there were ten. The machine used five at a time, so you pick five out of ten wheels, a set of ten wheels, and these were used lets say for a days key. Then you had a key tape for that day, and it was a numbered tape so you could start not always at zero, but you could start ~~anywhere~~ anyplace along this tape as long as you had enough tape left to finish the message. ~~and~~ Then there was the book of instructions and some auxilliary keying material that sort of made sure that the right wheels could

TOP SECRET

be put in the machine for each day's traffic, and the right tapes were choosen out of the supply of tapes issued with the machine. So we had the chassis, the wheels, the tapes, the book of instructions, ~~and then~~ the keying list which identified the wheels, and the tapes to be used for a given day over a period of time, say a year. Now Friedman's thought was that we ought to get cracking on the construction of these tapes, -- the preparation of these tapes -- so that when the machines came off the assembly line up at Wallace and Ternan, the complete package would be ready including the manuscript for the tape instructions and the auxilliary keys. Well I got stuck with the job of making the tapes because I had a little bit more practice in mechanical things than the rest of the group, ~~and~~ But I think they were smarter than I because they didn't let it be known, ~~and~~ so I got the job of making the key tapes for the M134. I might spend a little while describing the process. We had a tape punch. It was a keyboard device, ~~and~~ you typed on the keyboard with your fingers just like you would with a typewriter, ~~and~~ but instead of printing something on a piece of paper this punched a tape, just like you get, ~~with around~~ with hundreds of them around computer installations now. This was a ~~rate~~ rare thing. I'd never seen one until I was introduced to this program. Western Union had built several of them for use in the automatic tape transmissions areas around the country, ~~so~~ and this was a standard Western Union product. Western

Union also had ~~a~~ what they called a tape head which was a small box made of metal with a lot of wiring, a couple of strong magnets in it, and five little punches that would take the tape and read it. We called this the tape reader. Then we had a ~~tpae~~ tape duplicator, which was a product of IT&T rather than Western Union, and this would take a given tape ~~if you'd punched a tape would take the~~ tape that you'd punched and make another tape. And then we had a fourth device ~~which~~ that was a sort of haywire lashup of two of the Western Union tape readers which we called the tape checker. ~~and~~ You would take, for example, a master tape and pass it through one head, ~~in~~ and the duplicate tape, the tape duplicated, lets call it the slave tape for clarity, and you could compare the master tape with the slave tape to make sure that there was no missing ~~part~~ punch in the slave tape, and it was in fact identical, a 100% identical with the master tape. If there was a difference of one hole in any one of the levels of either of the two tapes the thing would stop and a little red light would go on, ~~and~~ Friedman was also planning to put a buzzer on it so you would also know about it by the bell ringing and the buzz buzzing. This was the tape factory and this was my baby. Probably one of the worst things that happened was the choice of the tape stock that was to be used for the key tapes that would be issued. Friedman had looked ahead and thought that the thin paper tape, which was used for ordinary message work and which at the most would be run 3 or 4 times and usually only once through the tape head, ~~and he~~

[illegible] COUNTY CLERK'S OFFICE
FOR CLERK

~~just didn't think this~~ would stand up. This was one of the problems with the ~~Vernun~~ Vietnam machine for example that made it impracticable, ~~because~~ if you looked at it it was a pretty doggone good idea from a commercial standpoint, but, when you used the key tape or the two key tapes, several times, they just wore out. The little reading punches, reading fingers, in the tape head would finally penetrate the tape stock and you'd get a false hole, ~~and~~ this created garbles. So we used a ~~read~~ Reed strong, and I remember it was kind of a grayish blue, slate blue stock, and it was real thick, ~~and~~ when it was put together they must have put some kind of an abrasive material in it, a fine powder or something, because in due course the tape punches, the little punches that automatically perforated the tape would get dull, they would begin to get tapered if you looked at them under a microscope, and they would stick and bind in the tape. ~~and~~ then you had to clean ~~up~~ out the head and put in new punches. ~~and~~ If you didn't have new punches you had to sharpen the old ones. Well, things went along pretty well the first few hours when we got started on the production program, ~~and~~ but within a couple of days, the whole thing bogged down because the apparatus just wasn't up to the standard of quality necessary to meet the requirements ~~in~~ of the system. ~~So~~ My job then sort of degenerated into a super maintenance project on this strange set of equipment which was not designed for the purpose it was being used, ~~and~~ As a result I had to sort

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

of coax out of this thing enough tapes ~~so we could~~ to make the initial distribution of the machines, ~~and this~~ I don't know that I ever was confronted with a more hopeless task ~~then~~ than making these devices work ~~and~~ to do what was needed, ~~and~~ I soon became desperate. It didn't take more than a month for me to realize that I was fighting a real losing battle here; and as you are apt to do in the case ~~of~~ where necessity becomes very evident, you try to figure out some better way of doing things, ~~and~~ I was dreaming about how rotors could be made to do other things than ~~and~~ decipher messages. I thought it would be a helluva good idea if we replaced these key tapes with a second set of rotors, ~~which~~ In effect this would generate five ~~screens~~ streams of impulses equivalent to the 'holes' and 'no holes' in the five levels of the tape and use this assembly of five additional rotors instead of the tapes. Well I thought this was a pretty powerful thing, ~~and~~ I just was so enthusiastic about it, because it looked like I was getting out of this impossible task, that I went to tell Friedman about it. It must have hit at the wrong time because it didn't ring a bell with him at all that day. ~~XXXXXXX~~ He said, in a very nice way, "Well, look Mr. Rowlett. We've got to have these tapes. We're committed, ~~so~~ please go on and make the tapes." ~~in a very nice way, and~~ So I went back to my tape factory ~~and~~ greatly disappointed, but the impulse to improve this process if any thing got stronger.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

Now I might talk a little bit about what ~~was~~ the difference was between the rotor concept that I was trying to sell and the tape concept that I was trying to get set up for. The preparation of the tapes involved, of course, a determination of something pretty much random which would be punched on the key tape that had to be duplicated and manufactured. Now how did we determine this? Of course it didn't have to be random, and this is a fine point in cryptanalysis. It just had to be unpredictable you see or extremely difficult to predict. Now almost any way you wanted to get a stream of unpredictable characters, ~~like~~ for example you could have a scrabble set. You could take the letters of the alphabet and just mix them all up equal frequencies, same number of A's, B's and so on, mix them up and then take the text resulting from a random drawing of these out of a hat and type it on the key perforator, ~~and~~ It would give you a perfectly acceptable tape. This is a great deal like you prepare one-time pad using digits. The idea was the same. Now the difference between this and my proposal ~~to use~~ of using the wheels, as I analyzed it, was that if you had the wheels and knew the alignment of the wheels then you could predict the key that was going to be generated by these wheels. Now this I thought was an advantage because you could then store a lot

of key in a few number of wheels just like you store a lot of substitution key in terms of the substitution wheel ~~and~~ also if you made this device in such a way that the two sets of wheels could be interchanged then you get a double advantage, as I look at it, my arguments then and this may be true or not cryptanalytically speaking, you get the double advantage that you get extra mileage out of your manufacturing process that produced the wheels. I didn't see anything wrong with it, and I could see a lot of advantages cryptographically as well as the personal advantage of getting out of this dirty job ~~that~~ I had, so I kept insisting that we pick this thing up and employ it instead of the key tapes. Well Friedman was most reluctant, I think for a variety of reasons, to go into this because we were indeed committed to the M134T1 and there wasn't anymore money laying around for the next version of it. Well finally in desperation I confronted Friedman. This went on for oh I guess six, eight, ten months, I confronted Friedman and said "Look, I'm just not getting anywhere with this. We've got to do something about a replacement for the tapes. ~~Their~~ They're not going to work. I know ~~their~~ they're not going to work because I've been closer to it than anybody else, ~~and~~ We just got to get something better and the only thing I know better is what I told you about, ~~and~~ Friedman was still reluctant and finally out of a real

fit of desperation I said, ~~either~~ either Mr. Friedman I don't know what I'm talking about, or I know what I'm talking about and you don't understand me. We just don't have a meeting of ~~the~~ minds and I think we got to clear this up because I'm going to have to quit that job. I just can't meet your requirements." Well he was real fussed about this because this was a hard spot and he just couldn't get around it on this confrontation, ~~and~~ so finally we took a couple of hours one afternoon and we went through it all over again; the circuitry and the controls, and the variety of modes that we could employ this thing and finally he agreed ~~well~~ that this ought to be given more consideration, ~~and~~ We wound up both of us very tired, ~~and~~ I think Mr. Friedman was real distressed about this turn of events because it meant backing off from something that he had sold real strongly. Well next morning he came in, eyes shining, just all excited and he says we're going to do this. We're going to do it, it's going to work, it's a beautiful idea, I'll see what I can do about getting out of the tape factory business, ~~and~~ Then he went up to see the chief signal officer with stars in his eyes to try to sell this new idea and the chief signal officer, who was great admirer of Mr. Friedman's, sent him down to see Col. Roger Colton who was the signal finance officer to see if there was money to develop this idea. Well Colton says, "Write it up Billy." So Friedman came back and we wrote it up and we

START 4

worked over the prospectus, what we'd have to do and what was involved and took it up to Colton. He had his so-called experts make a study of how much this would cost and came back and said, Friedman there just isn't that much money. We can't do this. It ~~will~~ have to wait for a couple of years because we don't have it set up in our budget, ~~and~~ Billy was very distressed and I think it's amusing to note too that he found out, as a result of this exercise and when the papers returned, for the first time that the $2500 that he thought he had for developmental work, research and development up at the signal corps laboratories had been expended on a field cipher machine for use out in the field under the direction of a mechanical engineer employed by the signal corps laboratories at Fort Monmouth ~~without any knowledge of this~~ without Friedman or the SIS having any knowledge of this at all. Colton and his finance people and the other research and development people had kept this a secret from Friedman and had gone ahead and backed the proposal ~~from~~ of the mechanical engineer. The money had been committed, ~~and~~ the device was about half built, this new field device was about half built, and Friedman still didn't know about it, ~~and~~ Col Reeder, Major Reeder at that time -- later General Reeder, ~~who~~ was also very distressed because

he felt this was not a good way to run a research and development project. Reeder was the assistant to the head of the war plans and training division so he was the number two man in the organization, and he got on this project, and make sure and I'm diverting myself a little bit from the ECM in this but I think its important to see what blocks were in our way when we tried to get a new and good idea sponsored by the fiscal people at that time. Unless you had pretty much the nod of the chief signal officer or the director of G2, things just didn't happen. It was kind of a personal decision at the top level and each one of the branches of the service. Well this was a very disappointing development and it didn't get me out of the tape factory business, and I guess about the only enjoyment I got out of it was in the drafting of the patent application to cover the invention so we could make an application for a patent to protect the governments rights. We didn't realize at that time that our own rights were protected, but we felt it was important to protect the governments rights, and so Friedman and I spent quite a bit of time putting the idea down on paper and consulting with the patent attorney. I think is Mr. Rowe was his name. I'm sure its in the history in the records of the SIGABA or the ECM, and I'm sure the files are there because I saw them oh about ten years ago down at the archives. Now, something else came along that was important

in the development of the ECM. I think I brought us up to the point of frustration. Now lets see if we can get the frustration out of the way. I lose my recollection of the time frame but sometime after the disappointment and after I'd produced enough tapes to satisfy initial distribution of the machines, the Navy in one of the rare periods of consultation between Navy organization and the Army organization -- I think it was Joe Wenger who told and it might have been Safford, but I believe it was Joe, I'm sure it was Joe -- Joe Wenger told Friedman that the Navy would be real disappointed with the Hebern contract and because the two machines, the Mark I and Mark II Hebern, had been unsatisfactory they now had a lot of development money but didn't have any ideas to invest the money in, and for goodness sakes did the Army have ~~something that~~ any good ideas at all. Well Friedman was pretty circumspect in this, and, before he talked to Wenger about the basic concept theory of the ECM, he got permission from the chief signal officer to reveal this to Wenger ~~and so~~ In due course the Navy was told about the rotor control concept for a cipher machine. I use that term to talk about the theory or theoretical concept. Now ~~this~~ things moved pretty fast just for a little while. Wenger took this idea, went back, came back in a couple of days with one of his collaborators, Friedman went over the idea again and discussed its potentials, its operation and the Navy boys went away. --

[redacted]

Wengert and his friend, ~~and~~ Then in about a week a whole drove of them came over. I think there were five or six of them, ~~and~~ They sat down in Friedman's office and discussed ~~the~~ this rotor control concept, ~~and~~ there were some nodding of the heads and there was some shaking of the heads, as I recollect, but there was certainly great interest on the part of the Navy folks who were looking at it, ~~and~~ then they went away, and ~~then~~ it got awful quiet for several days. I kept sort of bothering Friedman, "well, any reaction?" You see I had a sort of more than just a curiosity interest in this thing. I wanted to know what was happening to this what I thought was a very good idea, so Friedman asked Wengert and ~~he came back and~~ reported that Wengert had told him in response to a direct question that they were thinking about it; ~~and~~ that there were certain difficulties, operational difficulties, that they just weren't sure the idea would work. Well having gone through the experience of persuading Friedman I just didn't believe what the Navy was telling. I thought the doggone thing would work and maybe they weren't as smart as they thought they were. That was just my very bald, country boy reaction to this. How stupid can they get sort of? Now time passes on. The rest of the M134 tape control models are delivered to the Signal Intelligence Service, ~~and~~ I remember Major Reeder personally supervised the transport of these ten or twelve machines from New Jersey in an army truck down to

[redacted]

Washington, ~~and~~ he treated each one just like it was a baby in its cradle. ~~and~~ When he got down to the loading platform down underneath the wing ~~which~~ where the Signal Intelligence Service was located I was up on the third story, the third floor, looking down at the truck and watching the unloading process. ~~and~~ I saw Reeder get two stevedor types up in the back of the truck and he said, "Now we got to unload these boxes boys." This was in the summer time and the windows were open and I could hear his orders. So he goes around the truck and as he comes back around, one of these great huskies has got one end of the box and is getting ready to tip it over. Reeder runs throws up his hands and "Don't do that! Don't do that!" But it's too late, and the box comes down on its end. Oh what a crash. Now later on when we looked at ~~these things~~ the inside of that pitiful cipher machine, it was just as scrambled as you could imagine it could be, because it weighed something like 250 lbs packed. ~~and~~ The basket of the typewriter had fallen out, some of the solenoids had been jarred loose, the frame of the typewriter had been fractured, and it was a total mess. One cipher machine lost but something we learned. A valuable lesson. You got to build them rugged if you're going to have them in the Army. So it wasn't a total loss. Well anyhow we got the machines up and Friedman got ready to make a trip to Honolulu and to Panama to install the first

~~UNCLASSIFIED COMINT CHANNELS ONLY~~

~~TOP SECRET~~
~~COMINT~~

four machines. ~~We~~ He left it to us, Abe, Kully and myself and I got the brunt of this work because I was more familiar with this tape operation than anybody else, ~~so~~ We got the two machines working in the War Department code center. I had a third machine in the office that I used as a back up for the code center machines because every now and then we figured it wouldn't work and I wanted to know why this wasn't working to fold it back into the design of the next machine. Friedman was all for this. We were just together on this idea. Now Friedman gets his passport ready and gets his orders, ~~and~~ The machines are shipped, and when he gets word that they have arrived at Panama and Honolulu, he gets on a boat, one of the army transports, and he takes a cruise to Panama and he ~~sets~~ starts the machines working and we start communicating. We sent test messages; ~~it~~ That's the first step ~~to~~ in the introduction of the machines. This may sound foolish to a lot of modern day people, but this was really out in the wilderness for us. Nobody had ever done this before. Nobody had ever issued in the War Department machines to be used for enciphering messages, and the people in the coderooms were completely ignorant of what was required to make these things operate ~~technically~~ effectively. So we had to bridge that gap as well as to introduce the new machines. ~~and~~ Those of us who stayed at Washington did this for the coderoom and Friedman

was supposed to do it for Panama and Honolulu. Well to make a long story kind of a lot shorter, we got them working with the two places and Friedman started back home. Well it was about this time ~~we were working on~~ the B machine had been introduced and we were working on it, ~~and we were working~~ The Army group was ~~were~~ working very closely with the Navy group because when the B machine came in it replaced the old Red machine in great measure, ~~and~~ G2 and ~~O&I~~ ONI were very anxious for the decodes of this new system because with the introduction of the new machine ~~and since~~ we weren't able to read the traffic and we'd lost, among other things, the whole story of the tripartite arrangement which was being developed between Japan Germany and Italy, ~~and~~ that was of high interest, ~~and~~ we also knew from the Red traffic there was a secret codicil that had been formulated, and we suspected the terms of this secret codicil to the treaty was in the messages between Tokyo, Berlin and Rome, ~~and~~ so both G2 anx ~~O&I~~ ONI were very anxious for us to get on with this. Well ~~Hamm~~ "Ham" Wright and I used to exchange results more or less on a daily basis and we'd recovered the sixes with the Purple and we'd decoded these in a lot of the messages but we just couldn't decide what to do about the twenties at that point in time and ~~Hamm~~ "Ham" and I were speculating as to what kind of a mechanism the Japs could use. We understood ~~the~~ what we call the six mechanism. It was a pretty simple thing, but the twenty mechanism was a

great mystery at that time. Hamm I think was siezed by an inspiration. He said to me with a great big staring looking in his eyes, he said "I'll bet you the Japs ~~are~~ stumbled on ~~what we're putting~~ the principle that we're putting in our new cipher machine." and I said "Well, have you got a new cipher machine sort of?" "Yeah," and then he proceeded to describe the principle to me, ~~and~~ lo and behold it was the thing that I had shown Friedman as the replacement for our tape generating project and that Friedman had revealed to Wengert and the other people from the Navy, ~~and~~ Of course I was delighted, but I didn't let show through to Hamm that I was aware of these principles ~~because~~ since I figured ~~that~~ maybe "Ham" Hamm was a little premature in his revelation because the background that I knew that "Ham" ~~Hamm~~ didn't know. So after "Ham" ~~Hamm~~ left I sought out Major Reeder who by this time had become not only a very good boss but a very good personal friend and I told him about Hamm's story to me and reminded him that Friedman had revealed this several months earlier to the Navy. Well this amused Reeder quite a bit and he laughed and then he explained why he was amused about it. He said "I talked to Safford and Wengert ~~a few days ago several~~ a few weeks ago and they told me that they were just about to receive from IT&T the ~~product~~ pilot model of a cipher machine incorporating these principles and in Friedman's absence they proposed

that when he comes back and this device arrives they will have a demonstration for you and the Army, you'll be invited over and you'll take a look at it." and he says "Frank I'm going to make sure you go sort of," ~~and~~ so far as I was concerned that closed the episode because there was no point in pursuing it. I was satisfied that the Japs though were not using this principle because I knew enough and had done enough tests on it that and as a matter of fact I had run this thing against the text earlier before Hamm had proposed it because it was so close to the top of my mind I just couldn't avoid making the test really.

typewriter and typists to do the manuscripts, at least the first manuscript, and then the sorting well, then as we went from one code to the next code that is we took the MI11 and wanted to construct MI12 it meant a realignment of the plaintext elements with the code groups and thus we had to make a scramble, a new scramble of the relationship between the code vocabularies and the plaintext vocabularies. This was a very onerous task and had to be done cleverly so there was no system or rhyme or reason that could be used by a cryptanalytic organization who might undertake the study of this code to their advantage. I dont remember the exact date that we were invited over to the Navy to see this first model of the new device, but I believe it was within a couple of months after Friedman's return. He and Sinkov and Kullback and I were invited over to the Navy where they gave us a demonstration of the device, and I must say ~~that~~ I was personally real gratified when I saw the theory put into hardware. It was a much better device from a design and construction standpoint--much more rugged, much more reliable than the M134T1. The keyboard, for example, on the device was specially built, modification of the teletype IT&T 15 keypunch. The rotors were well built stainless steel parts were in them. This the Navy required for operation on the battleships. The electrical components were first class for those days. The contacts -- ~~are~~ a very difficult part of a cipher machine are the separator contacts that operate between the moving rotors ~~and they'd used a good~~ were well designed. ~~in these and~~ It was a most beautiful thing to look at from where I stood and I couldn't keep my hands off it. ~~and~~ Of course the Navy was

delighted to find somebody as enthusiastic about it as I appeared to be. Well we spent, I dont know, I lose all track of time but I think it was a couple of hours just looking at this and talking about it. One of the things that bothered me a little bit about, as I look back is the Navy's incorporation of an extra set of the 10-point wheels in front of the two sets of wheels, one set of which ~~one set~~ provided the substitution maze as they called it and the other the control maze, ~~and~~ I was very curious about the circuitry that they'd decided on in terms of the association of the contacts on the end plates ~~plates~~ of the control maze with the stepping magnets of ~~the~~ both mazes. Of course, the stepping of the first maze was metric and required no vertical control, but the stepping of ~~the maze which~~ thing the wheels which comprised the substitution maze was a critical in the whole concept and that, of course, was achieved by the circuitry through the control maze. As I recall the machine and look at it, the design of the stepping mechanism was far in advance of the stepping mechanism used in the M134 that Friedman had just distributed. In the Army 134, a single solenoid was energized ~~is~~ and the energy stored up in the solenoid then kicked the wheel forward. If the spring got weak or the voltage dropped off, sometimes the magnet would not ~~energize~~ store up enough energy to push the wheel forward, ~~and~~ If the contacts wheels themselves got a little gummed up then the resistance of the wheel would overcome the push of the solenoid and you'd get an operational failure. The machine built by IT&T for the Navy had a positive mechanical drive with only a trigger operated by the electrical circuit and this trigger could be adjusted so that ~~its~~ it required only a little bit of energy, and

TOP SECRET

~~that~~ it wasn't apt to gum up like the wheel in the Army device, and this was a beautiful thing to contemplate, ~~and~~ I think in the IT&T model that they produced for the Navy they used real forward looking engineering, and I can remember the feeling that look we are ahead of the rest of the world in cipher machine production. This is beautiful. Mechanically we're good and of course I was convinced that cryptographically we were good because there it was, the idea you see, right in the machine. Well there wasn't much we could do about this machine, nor was there much we wanted to do about changing it because the work that had been done engineering wise was very good application of the principles. We didnt see, though, the advantage of the extra set of rotors that the Navy had introduced for Army purposes. We preferred a plugboard. The Navy for some reason didn't like plugboards, but this was not a point to ~~this was not a point to~~ quibble about. Now I'd like to go a little bit further down the historical path of this thing. I think from this point on in the story of the ECM or the 134 is pretty well documented. I think it was a wonderful thing, almost a miraculous thing, that through the accidents I've described here, the Army and Navy decided to have a machine that would be used by both that was identical in chassis, identical in operation and which permitted through the issuance of differently wired rotors to the two services sort of a three-part concept, operation, for example, using the same chassis the M134T the chassis ECM we called it the M134T1, 2 or 3, I don't remember what type it was -- probably type 2 and type 3 came on later using that same chassis with a rotor of the nature the difference between rotors being the wiring

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

of the rotors and you could have just as many different wired rotors as you want and they'd all work in the machine. The control rotors were interchangeable with the substitution rotors. This was an advantage and it made both the operation and the construction of the machine acceptable to both services. But now this is what resulted. The Navy could, by having its own set of wheels, have privacy of its own communications within the naval service. The Army by having its own set of wheels could have privacy of communications within its own services. They could extend the use of this machine down through the echelons without either jeopardizing the Navy messages enciphered by the machine, because they used different wheels, and likewise not having its own communications jeopardized by the Navy's use and indeed misuse because the principle was so powerful at that point in time that our cryptanalytic capability wasn't affected by it. I mean, it could resist everything we knew at that time. Now there was a third domain of advantage, and this was in terms of joint communication between naval elements and army elements. Of course the Air Force not being separated off from the Army at that time, there was no third service communication requirement needed. Now there was another sort of advantage that if you wanted to use this machine for the War Department command network you could have a special set of rotors wired up for the War Department command network, then for the next echelon down you could have a different set of rotors so that you maintained the integrity of the communication of the relative echelons of commands both in the Army and the Navy as well as the joint communications, and this was a most persuasive and

TOP SECRET

forward step I think in practical cryptography because before you had to have a different set of codebooks and these became onerous -- but here are just little packages of rotors was all you needed with a little pamphlet that told you how to use the rotors and so the concept was indeed very practical. Now when we begin collaborating with the British there was a third advantage which came out and the British used the Type X. It was not a very practical machine. It wasn't near the slick article that IT&T had produced for the Army and Navy on this joint contract that ultimately came out, and I remember setting in with the Navy and with the British communicators and trying to determine what kind of a cryptographic system would be used for combined communications between US forces both Army and Navy and their opposite numbers the British. The British openly proposed the Type X. We did not propose the ECM on orders from high command both in the Army and Navy. That we would look at their devices but we would not tell them about the ECM, and this was prudent, and I believed that this was a good decision because we had watched France, and we didn't want, by revealing our device to the British, to jeopardize the security of the ECM by spreading the knowledge any further than we had to. I think we got a good, and neat solution to this because by a slight modification of the control circuit in our ECM we could make it duplicate the Type X, so we accepted the Type X for combined communications with special rotors but we postulated that we would use our own modified machines, which the British could not have access to, in our code rooms and they could use the Type X. In other words, we could take this ECM and convert

TOP SECRET

it and duplicate everything that the Type X (could do) and actually it was a more efficient machine than the British Type X. Now let me sort of philosophize a minute here because I don't know whether anybody else saw this as vividly as I did. But if I think back at what a conglomeration of a mess we would have had if we had to war a Navy machine, which was one type of machine, and an army machine, which was another type of machine, we'd probably have to have a third machine which would be needed for the joint communications and then when we got into the combined communications with the British I don't whether we could have modified one of these machines or what kind of a thing we'd have had, so I think it was just a real heavenly miracle that the decision was taken when it was taken for the Army and Navy to use the same machine. I thank the Lord that we collaborated in the production of this thing, and I'm quite sure that one of the contributions that the Signals Intelligence Service made to the winning of the war, World War II is found in the good sound cryptography that developed and which was finally realized when the machines were put in use. And I think there was one side advantage of this that probably has been lost sight of. In our arrangements with the Navy to have the ECM bulk-produced the Navy, who let the contract, wanted to get the devices out to the fleet and naval stations on shore so they had planned to take the first output of the assembly line where these machines were being built. The Army was going to take the second batch. I don't remember how many was in the first batch but there was enough to satisfy the Navy requirements and then the Army was going

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

equipp each division, and the War Department command circuits, and related circuits with the second batch. Now just about the time ~~they were coming off,~~ the first models were coming off the assembly line is when the Japs hit us at Pearl Harbor. The Army mobilized overnight and there was an urgent need for cipher machines. There was a batch of cipher machines sitting there with Navy nameplates on them. The Navy didn't need these machines so agreement between the Army and Navy was to flip; ~~and what they had to do to put into effect this change in plan,~~ the flip namely being that the Army took first batch and the Navy took the second batch of machines. All they had to do was two guys, one with a cold chisel, a small chisel and a hammer and he went down and knocked the nameplates off -- -- and the second came along and put the Army nameplates on where the Navy nameplates had been removed. Now this is a piece of luck that you really don't deserve. But we had it and thank the Lord that we did have it because if we'd had those separate machines the Army might not have had machines for its division until it was too late for them to be effectively used. Then we would have had another repetition of what I'd like to tell as the SIGCOM (SIGCUM) story. It might be important at this particular point to make a comparison between the status of cryptography with reference to cipher machines in the various nations. I mentioned the British Type X was ~~far beyond the was~~ far below the beautiful model produced by IT&T. Let me talk a little bit about the Type X. Type X was a modified Enigma if you look at it substantially. The greatest advantage that the British had incorporated in it was that it had wheels with a double row of contacts. Just as the telephone company uses a double contact

TOP SECRET

to insure positive operation of the relay, the British applied this prinicple of a double circuit through to the wheel to insure positive operation of the wheel contacts because they were the greatest source of trouble in a rotor machine. That is, the contacts provide quite a bit of resistance build up in a small voltage traveling over a circuit that passes through a bunch of contacts that may become dirty overnight, particularly if its in an area where there's quite a bit of moisture, smog and sea water, so the British had built this mechanical or electrical advantage into the machine, but its motion was a great deal like the M134T1 that Friedman had distributed, ~~and it was not~~ I think they were about equally reliable because we did use the M134T1 effectively as a backup system in the War Department command net for special communications with the intercept stations, ~~and~~ in fact the last ~~message~~ intercept message that was sent from Corregidor was enciphered in one of the two machines that Friedman took out when he first distributed the M134. Now what were the Germans using in that timeframe? They used the Enigma. We ~~had~~ were not unfamiliar with the Enigma because, as a part of this cryptographic purchase program that had been set up when the Signal Intelligence Service was first organized, we'd gotten a copy of the commercial Enigma and we understood it very well. The military and naval in our Enigmas we finally discovered being used by the Germans were some improvement over the commercial Enigma. Cryptographically they were much better because they had this plugboard arrangement, and ~~so~~ you could vary from

[redacted]

day to day the relationship between the contacts of the keyboard and the input and output ~~[illegible]~~ end plate on the rotor maze. The control principle of both the Type X and the Enigma, all being rotor machines of course, the Type X and Enigma both used mechanical key generator. The key was mechanically generated and pretty much a modification of the metric ~~step~~ stepping, the same you get ~~on your~~ in the odometer on your automobile. This of course could be varied so you could have two wheels which I believe the British had achieved in the Type X. The Germans had their own special way of working this but it was totally predictable and built into the machine. Compared with the ECM and its control maze the motor key was much more flexible in variation and ~~it~~ was limited only by your wheel combinations that were set up ~~and~~ in the wiring of the ~~inplate~~ end plate in the control maze. The order of security was much greater so far as the motor key was concerned in the ECM than it was in the Type X or the German Enigmas -- I believe even in the best models which were used by the German navy. Also the ECM had the advantage that you could sort of build in the mechanical motor key which duplicated the Type X, ~~and~~ we actually converted some of the ECMs to do Enigma work ~~because they~~ if you had to decipher an Enigma message. The British didn't of course have any device as versatile as this ECM, ~~and~~ they used their own modified Type X's. I remember seeing a battery of them at Bletchley Park when I inspected the Bombe installation and the decoding section they had there. The Bombe installations were separate. But most of the decoding was done in the German military and air sections at Bletchley. Now lets take a look at the Japanese machines. The Japanese machines were generically different ~~from~~ in the cryptography they employed from either the Type X which was an Engima type. the Type X and the Engima being pretty much comparable,

~~[illegible] CHANNELS ONLY~~
TOP SECRET

~~and~~ The ECM ~~which~~ was more like the [Type X] than the Enigma but with greater advantages built into it. The Japanese machines, the ~~Red~~ Red machine, and the early on version of the Navy machine which enciphered the ~~Kana~~ kana used what I think can be best described as a half ~~Hebron~~ Heburn type of wheel. Let me explain that a minute. A ~~Hebron~~ Heburn would if you look at it if you take a ~~Hebron~~ Heburn type wheel and slide it between two ~~a~~ end plates will produce sort of a substitution square. Now this substitution square can if you will cryptanalytically or cryptographically or cryptologically be replaced by two ~~viginere~~ Vigenère squares; the result of the sliding of the two series of contacts one on each face of the wheel against the ~~in~~ end plates, so ~~Hebron~~ Heburn then, is really a double ~~viginere~~ Vigenère substitution. Now in the ~~Red~~ Red machine and the early Navy machine there was a commutator which effected a substitution ~~which~~ that could be exemplified by a simple ~~viginere~~ Vigenère square. ~~So we called~~ For a lack of a better term, and because it was a very descriptive term, we called the commutator used in the Red machine and the early Navy machine a half ~~Hebron~~ Heburn substitution. Now there were two commutators in the ~~Red~~ Red machine. There was a small one for the six that had six contacts, and a large one for the twenties. Both these were linked mechanically so they could not get out of step, but the mechanical linkage was driven by what evidently was a pin wheel of some sort ~~a motor wheel with the Red machine~~ within the ~~Red~~ Red machine the motor wheel afforded was basically a 47-point wheel and certain of the pins or certain of the positions on this could be varied either to produce a step or to skip a step. ~~and~~ This is what interrupted the movement of the ~~viginere~~ Vigenère or half ~~Hebron~~ Heburn type commutator to produce

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~TOP SECRET~~

the substitution. It was a very simple concept and was probably not as good as what we found in the Kryha if you examined it carefully. Now the Purple machine was a breed of cats entirely different. We'd never found anything like it in the literature. There was nothing like it in the machines. The Enigma was entirely different. What the Japs had done evidently was to use the concept of employing telephone relays. That hadn't been done before. We never thought about. As a matter of fact I didn't know about telephone relay until Rosen brought it in and said why don't we use one of these to effect the substitution for the sixes on the Purple machine we're building. I'll tell it in the Purple story but we just didn't know about telephone relays until we'd actually gone deeply into the solution of the Purple machine. Telephone relays and the stepping relays in the sense that they could provide a cryptographic mechanism. Now the Japs then I think were in a completely different concept with their Purple machine than the rest of the world because we had pretty much tied ourselves to the rotor concept. The Japs evidently didn't like rotors or didn't know about them because they never used them. Now there was another machine, the Hagelin machine, which was a straight mechanical device. The Damn machine was a failure because electrically wasn't reliable. So Hagelin gambled strongly on the development of this device. ~~We bought a whole bunch of them for use as a~~ We bought the rights from Hagelin, I think the US government did and we had one of the typewriter concerns up in New England build a whole mess of them. I believe they're the 209s. That was about the state-of-the-art in cipher machines around the turn of the '30s into the '40s. I'm real proud though that the Navy got IT&T to build the ECM because it worked throughout the war and was most reliable. I think we had the best

cipher of anybody. ~~The Hagelins ~~they used them and electrically I mean the Italians I'm sorry~~ The Italians used the Hagelin principle except it was motor driven, the machines were motor driven instead of crank driven. The Kryha machine never really nobody ever used the Kryha I think it was used for some German communications but they weren't very important.

Q: (Vinci) Was the ECM ever used for non-military communications? Diplomatic?

A: No. Actually if you look at WWII the main communications in the diplomatic fields were between London and Washington. ~~and I think there was some use, well~~ diplomatic communications don't amount to much in war time. They're great things in peacetime, but ~~when~~ during the war most of your diplomatic work just naturally ~~falls~~ fell under ~~the~~ military considerations. ~~and so that~~ The bulk of communications between Washington and London were military -- between ~~I mean~~ Eisenhower and George Marshall.

Q: (Hantz) Did the President use the ECM?

A: Not in the sense that the President personally typed the message but his messages were all encoded in the ECM. The ECM was ~~looked at,~~ looked upon by both the ~~A~~rmy and the ~~N~~avy as the ultimate in US secure communications during ~~WWII~~ World War II, and naturally it carried the best -- the most secret traffic. Some of the Roosevelt-Churchill conversations and some of the high-level military communications were carried by the SIGSALLY. This is that special voice encipherment system that was set up by ~~B~~ell Telelphone between the Pentagon and the ~~War~~ Room in London and, of course the advantage there was to be able to use the telephone securely. The Germans never really got on the the SIGSALLY. It was well ahead of its day. I think Bell Labs did a magnificent job in coming

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

up with what they did at the time they did.

Q: (Voice) Did we assist with that at all?

A: Yes. From the standpoint of the cryptography we had and this was the Signals Intelligence Service, Leo Rosen and I ~~were to~~ worked with Bell Labs in analyzing and assessing the security of this thing. It was good. The security was good, ~~and~~ We made some nasty remarks about it but we didn't really have any thing to add to the security because what they did is they used a random noise source which then was mixed somewhat along the ~~Vernam~~ Vernam principle with the voice channels and so you got a real good encipherment. It was one-time key really and they had ~~had~~ to have a bunch of plates cut ... platters cut ... and distributed them between Washington and London. These were the two centers that SIGSALLY serviced. All other communications with North Africa, for example, and with Australia went through the ECM, that's both Army and Navy -- the separate channels. ~~And~~ This is an example of what a wonderful thing it was that the Army and Navy used the same doggone machine. New paragraph. One of the problems which was always with us during the 1930s is how the Army and Navy should work in collaboration in both the fields of intelligence production through cryptanalysis and improvement in the of ~~the~~ cryptographic systems so that the US services, ~~through~~ the two military services and hopefully ~~this would spill over into~~ the (State Department) DoS which were the three major users of ~~the~~ combined cryptography in those days, would have the best ciphers systems that could be achieved in that time period. This was a fairly difficult problem for both sides because while on the technical level there was a great hunger for the

[redacted]

expansion of knowledge through exchange of ideas and discussions as well as exchange of results. This hunger was not fully appreciated by the more or less politically minded upper echelon Generals and Admirals. This showed through very vividly in connection with the collaboration on the Japanese problem itself. Early on in our work in Japanese the Army and Navy had tackled the Japanese systems. The exploitation of Japanese diplomatic ciphers, so far as the two- and four-letter codes which were used unenciphered or un-transposed in those days, offered no problem but was really a magnificent training exercise to lay the groundwork for the more exacting responsibilities which developed when the Japanese began to improve their cryptography. The problem though which arose, the vexing part of the problem was soon developed when the Army and Navy began translating the same messages and different versions of the same message would go from G2 and ONI to the same recipient, [let's say up in the State Dept.] There was a great bit of acrimonious discussion which resulted from which was the more reliable the Army translation or the Navy translation. Which version was more accurate? This bothered those of us who were in the technical end of the business because we did not have any competence in translation. We could recover codes and recover keys and decode messages and we could turn them over to the translators who would reduce them to English. But whether or not this was an accurate translation sometimes became a moot question because Japanese in itself is a most difficult language to set over into English. Johnny Hurt used to make a statement that I carry with me and I think is pertinent now that the best you can do in translating a Japanese message is to

DoS

[redacted]

TOP SECRET

make a commentary on what the substance of the message is. You can not do a word for word translation but you can describe in English what the Japanese text is trying to convey if you're dealing with a message or a letter or a newspaper article. So according to Hurt's philosophy as I recollect it, Japanese would be a very difficult language to make sort of accurate, verifiable translation of. The accuracy of the translation depends on the translators understanding of the subject matter which is being discussed in the message. This becomes probably more of a problem in Japanese than it would in German or one of the Romance languages. Now this problem became aggravated when the Red machine was solved. I think I mentioned earlier that the Army had made the initial break into the Red machine and we'd started into production on it and were feeding translations to G2. In our developing collaboration with the Navy, we had, of course revealed to them what we had found out about the machines, and remember ~~there is a very strong motivation on the part of the Army,~~ there was a very strong motivation on the part of the Army and at the same time on the part of the Navy -- call it patriotic if you will, but it was there to keep each other informed. Since we were both Americans and since we both were sister services, ~~that~~ it was in the common interest to exchange anything technical... any knowledge about the operation of cryptography of a foreign country because this might develop in some other aspect or context, maybe in a military system or a naval system or a weather system or an air system used by a foreign country, ~~so there was a great motivation, call it patriotic if you will, but it was there to keep each other informed.~~ So this sort of acrimonious attitude that developed from the comparison of the

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

translations was a little bit distressing to us But we didn't concern ourself too much about it because our concept of translation was that lets translate this in the Army and the Navy and then lets pick the translation which sounds the best, most plausible and most in line with what the message really says because of the basic difficulty of making the translation as Hurt described it, and let that stand and let G2 and ~~O&I~~ CNI resolve this problem themselves. Now the problem in the Army was a little bit different from that in the Navy because the Navy translating people were the type that Kramer represented. He was a very good Japanese scholar and most of the evaluation of the contents of the naval messages were done by ~~Japanese trained~~ Japanese language trained officers. There weren't as many of these in the Army as we needed ~~and~~ so instead of assigning these to G2 we brought them up to augment the Army translation staff. ~~and~~ The evaluation then was done by the desk officers in G2 who might or might not be knowledgable in Japanese. Well, the intelligence which we developed out of the Red machine solution was of such a high quality that the Navy felt that this was no longer sort of a training exercise ~~and that~~ G2 likewise felt the same way, ~~and~~ We were now getting intelligence of such importance that they could begin to develop some kind of a picture about the Japanese. There was a very able officer by the name of Col. Bratton in G2 who probably contributed more to this concept than any previous officer we'd had. Bratton was Japanese trained, he was intelligence trained, he was a fairly senior

TOP SECRET

officer, he was a full colonel, and spent a lot of time in the Orient and probably had a better understanding of what was required than anybody else in G2 or in the War Department at that time, ~~and~~ I can remember Bratton coming up and being in the office, standing outside the vault door out of which we operated, before I got there early in the morning ~~to verify a translation, and~~ to verify a translation. The specific one I remember dealt with the tripartite arrangement between Japan, Germany and Italy and it was the first announcement of this, ~~and~~ Bratton was terribly concerned about the implications of this for the obvious reason that when the Japs and the Germans and the Italians all got together it meant something pretty formidable that the US would be confronted with and ~~the~~ their war plans would have to be examined. The whole posture of the US military might be affected by ~~it~~ this diplomatic development. Now, as we see ~~now the importance of~~ the contents of these messages becoming more and more ~~exemplified~~ important and of greater interest ~~in~~ to the upper levels of both services ~~and that the upper levels of the Army and Navy were aware of it and we find that now in time that these items of intelligence are becoming of~~ not to mention interest at the Presidential level and at the Secretary level in the State Department, we find another development taking place namely, this old competitive attitude between the Army and Navy and who gets the credit for it if you want it ~~to~~ put ~~it~~ bluntly. I can remember once when I took leave, I was gone for about three weeks and before I left we had successfully predicted all the Red cipher machine keys for a year ahead, ~~and~~ I felt ~~well~~ that the work load is diminished and before I get on another project I had better

DoS

get my leave in because I lose it if I don't. So I took leave and when I left the pot had begun to boil in terms of who gets the credit for these messages, who really broke this. We felt pretty strongly about it because Kullback, Solomon Kullback and Frank Rowlett had made the entry into the Red machine and it was Army property. The solution to the Red machine was Army property. Although we've got to give some credit to the Navy for telling about the cryptographic instruction of the Japanese naval machine, which the Red machine was a prototype. But the simple fact is that the Navy had not read the Red machine and they'd had ample opportunity and intercept to do it, but because of their preoccupation with the naval problem had not paid sufficient attention to the diplomatic problem to carry on this next and, as it turned out, ~~be~~ very feasible step in working on the Japanese diplomatic traffic.

This point was appreciated by the folks on the top echelons of the War Department and made a big issue of in their arguments with the people on the top of the echelon of the Navy Department as to who should get credit. I think it's pretty obvious that the Army wanted credit for the whole kit and caboodle and the Navy couldn't tolerate this ~~and so there was a good reason, and~~ I can side with both because I don't think it really made any difference who got the credit as long as the word got up to the people who needed to have it. But evidently it made some difference somewhere in the Navy, maybe before it got to the Secretarial level and in the Army before it got to the Secretary of War. So when I came back from leave, George Bicher ~~Beecher~~ who was one of

[redacted]

[redacted]

the military students assigned met me almost at the front door on the first morning I came back and he said, "We've got a terrible mess on our hands. ~~We've~~ It was decided while you were gone that the Army would send the translations up one day and the Navy would send the translations up the other day, ~~and~~ They drew straws to see which service would get the odd day and the even day and it was decided. But it doesn't work because what they're using is the date that the message was translated and we still got this duplication of effort. How do we solve it?" This may seem absurd but I think it does demonstrate sort of the lack of understanding of the technical aspects of the kind of work ~~that~~ we were doing. ~~and~~ We finally concluded that, since the Japanese changed their key on a 24-hour basis, at midnight, ~~that any key which was that~~ any message which was applied in the key for the calendar day listed in the Japanese code instructions pamphlet, ~~and~~ then that was the proper cryptographic date of the message and that would also be considered as the origination date of the message. ~~and~~ Then we would have another little box down on the corner of the translation which said "date translated" because that could be anywhere from twelve hours to twenty-four months away from the cryptographic date of the message. Well if it had not been for this nicety of the Japanese changing their cryptographic date of their message at 2400 we wouldn't have been able to resolve this problem between the Army and Navy as to who gets credit for the delivery or production of the translation. I think it is also a sad commentary on the people who received the message who thought there was some special magic that the Army

or Navy had which permitted them to produce a message only on an odd or even day. I have never resolved this absurdity. I apologize for bearing down so hard on this odd-even day thing because it may seem trival as we look at it today but at that time it was happening it was a big issue and I think it gives a pretty good example of just what the climate was at that time in terms of collaboration between the Army and the Navy. Actually these problems were not real problems in terms of what was going on in the more technical aspects of the work because there was this strong motivation on the part of each to keep the other apprised of anything new that was developed. Another difficulty we had which had to be surmounted was the reluctance of either service to disclose its cryptographic principles to the other. The Navy however I think showed the wisdom in calling on the Army for consultation purposes when it approached Friedman in terms of the testing of the Hebrew principles and I think we began to realize that we had to exchange information and assist in that kind of a fashion if we were to do the best kind of a job we could for the country. So this soon became accepted as a principle of collaboration. Now one of the examples of collaboration between the Army and the Navy that I think might be considered for a minute was the development of the strip cipher as a joint system. The Army used codes mainly in the early '30s about 1935 I would say is the time frame and the Navy had certain cipher systems and code systems which they used for the fleet and shore installation communications. Now to develop a system that could be

TOP SECRET

used and totally viable for joint use between the Army and Navy was one of the problems we had to solve. This was done by a sort of conference at the technical level between Friedman who headed up the Army side and, I believe it was I don't remember who was on the Navy side, I don't think it was Wenger in this instance, but as a result of this it was decided if we could take the M-94 which at that time was authorized for Army use and make it more secure that something like that might be a good thing to use for joint communications. However, our work on the M-94, in our research as students in the Army, had convinced us that it was not a proper cipher to be used and should be rejected and eliminated from our communications security usage as soon as possible, and We were most reluctant in the Army to propose and accept this as a joint communication because we didn't want to continue to use it, and We were afraid if we accepted it as the joint system that it would be perpetuated unnaturally beyond its already too long a life. I think it's pretty obvious that the strip system came out as a more or less automatic result of these discussions about the M-94 and the need for joint system. I remember that we collaborated in the development of the strip cipher device. Some of the early models of it were made out of plastic covered paper and these were not very good. The strips were thick, about a 1/16 of an inch printed at the Government Printing Office and overlayed on cardboard stock which was pretty fragile, and if you started shoving these strips up and down in the holders they'd break, and pretty soon you had an inoperable

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

system. Seiler and his group over at the Naval Gun Factory had some milling machines they used. ~~and~~ They took some aluminum sheets about 1/4 or 5/16 of an inch in thickness and big enough to hold 15 strips and build out some dovetail slots that would accept a strip of paper. ~~and~~ This looked like a pretty good device. Another approach to it was to rivet some round bars on a metal plate big enough again to guide the strips. These didn't work so good because unless you had rivets all the way down the bar, and we could visualize only three or four rivets, every now and then the strip would get caught under the bar, wedge itself in, and you'd ~~try~~ feel the strip and again the device became inoperable. Finally some molded bakelite bases were made and the system then began to reach the realm of feasability, ~~and~~ It was in fact adopted by the Army and Navy as a joint Army-Navy cryptographic system. Now this was a healthy thing to be confronted with a problem and have to solve it jointly; ~~and~~ to put the joint resources to work and to get a successful solution was encouraging. ~~and~~ This meant a step closer together between the Army and Navy at least so far as the technical people were concerned, and I think probably was a very useful thing in laying the groundwork for the later collaboration and adoption of the ECM when the time came for that decision to be made. Other aspects of collaboration where we ~~began~~ begin to work together was found in the intercept. The Navy had some considerable facilities in the Far East and we were trying, and they were intercepting both diplomatic ~~phrase~~ ?? from diplomatic net. They had the best coverage possible from it, and we were trying to develop some military intercept, intercept ~~from~~ some Japanese military messages

** TAPE #3 Side one - almost at end of tape

from Manila and without success. We didn't realize it at the time but it became evident later that you have to send a message before you can intercept it and the Japanese military just weren't sending any messages. They didn't have any need to in that time in history although when they began the invasion of China later on why there was a great rash of Japanese military messages suddenly blossomed up. Of course when we saw this happen we realized why we'd been unable to intercept Japanese military messages in the earlier years. So this collaboration sort of dividing up the intercept field without total commitment to responsibility mainly as a friendly arrangement rather than a hard and fast arrangement I think showed also another step forward in collaboration. We're now reaching the point where about the time the Purple system came into being we find that the Army [and] Navy, so far as the Japanese is concerned, are producing translations on an odd and even basis. There is a complete change of technical information, cryptanalytic intercept and the other important materials of exploitation and a fairly friendly and rested and easygoing relationship between the technical people. A little bit of trouble began to emerge shortly after the introduction of Purple. I saw this pretty clearly because when the new machine, the B machine was introduced in March whatever year it was which slips me for the minute, the Navy was as much interested in breaking into it as we in the Army. I think the Navy kind of felt like well the Army scooped us on this Red machine lets scoop them on the Purple machine and this

* End tape 3, side 1.

~~TOP SECRET~~

was terrific because it stimulated both of us to lot stronger effort than we might have made if we'd been operating without this competitive spirit. The first appearance of this change in attitude or change in philosophy came after ~~through~~ the Purple machine had ~~that~~ resisted our solution efforts for about 4 or 5 months and the Navy began to get pressure -- I believe this was about the time that ~~they~~ Admiral Redman was beginning to make his influence felt strongly in the Navy and the decision was taken that any effort which remained over and above what was required for work on the Japanese naval systems could then be applied to the diplomatic. Now as you begin to work on the cryptographic system and you know more and more about it, you find that you need more and more help on it. ~~so~~ If you begin to get a break for example in the navy system with this sort of greater urgency on naval problems you, if you were in the navy -- would then tend to break away from the diplomatic and first thing you know the diplomatic effort is just atrophied, I guess is a good word for it, to The point of where you might as well break it off and not do it. I think there ~~it~~ was an interesting sidelight on this that I might bring out maybe when we talk about Purple, but we found that the Navy, along about six months after the B machine had come into effect, had sort of decided that it was no longer an important thing for them to work on. ~~and so~~ They turned away from it and went to work on the navy ciphers. Well, this bothered us in the Army a little bit because we kind of felt like that maybe the easiest way to get into some of the naval systems was through solving this new machine. ~~because~~ It was a good machine and

~~TOP SECRET~~

TOP SECRET

they might be using it in the Navy and it seemed not to prudent, at least that was my attitude, for the Navy to drop its effort. That was the Navy decision and they did. We didn't argue too strongly against it because then we would have been meddling in Navy policy, and this was against the ethics of the Army and we were charged not to try to-- well, to avoid any meddling if we knew how to do it. I think from this point on until we revealed to the Navy that we'd successfully broken the Purple machine in the Army, the situation tended to get a little worse. But it took a sudden turn within days after the Navy discovered that we were again into the main stream of intelligence between Washington and Tokyo and the other holders of the Purple machine and they felt a strong compulsion to get back onto the diplomatic traffic in full force. This continued until Pearl Harbor. The Navy effort from that time on on the diplomatic remained as great as was required and I think an example of their increased interest in diplomatic traffic is found when they called in some reservists - this was the Frank Raven, George Lynn, B, the Brotherhood group, who were put on the watches over in the Navy to make sure that the Navy was doing at least its share of the traffic and were ready to do more. Of course we had augmented our effort in the Army because the traffic was much more valuable from an intelligence standpoint since now we were delivering it to the President, G2, and the State Dept, Secretary of State, and everybody was, this was a big deal of the day for them to see what the Japanese were saying to each other. The interest that was generated there was reflected back

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

into the working circles in the sense that we moved things faster, we got intercepts in faster, we turned out the translations faster, and we screened the traffic looking for interesting items. I say "We", I mean ~~this is~~ these are the people in G2 and ~~O&I~~ ONI as well as the cryptanalytic organizations who made sure that those items in which an interest had been expressed ~~in~~ on the State, Presidential, and Secretarial levels ~~made sure that they~~ ~~it~~ got up there just as quickly as they could, ~~and~~ In fact it was in this period I remember two things that are worthy of mention. One, for one year I think there wasn't a single Japanese diplomatic message that we'd intercepted that we couldn't read except two, and I believe these were one of these was a numerical message which was addressed to Hanoi and I think the reason that we didn't read it was that the intercept operator made a mistake and typed in the wrong heading on it, ~~and~~ It was a maybe a French or Spanish message and obviously Japanese codes wouldn't work on that. ~~We~~ We also had a little batch of traffic that was just so badly garbled that you couldn't tell what it was, ~~and~~ But even some of this ~~we had~~ ferreted out and gone in the middle. We'd lost the heading and the beginnings and endings and just little stretches in the middle that the intercept operator had sent in and we liked for them to do this because we might miss the heading at one intercept station and pick it up at another, ~~and~~ There by patching the two together you could come out with a complete message. So we encouraged the intercept stations to do duplicative work, (to get back) but there was just a trivial, microscopic amount of -- I'd say less than a message that we failed to read in one year, ~~and~~ I did

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

TOP SECRET

a little work on this to see if there was in fact a message that we hadn't read and these are the results of that survey which was stimulated more by curiosity than necessity. Now we also made arrangements in that time frame to get the messages directly from the cable companies in Washington, ~~which had~~ The Japs would ~~come~~ filed their messages to be sent to San Francisco by landline, and then in San Francisco at the commercial radio station they'd be put on the air on a regular schedule and would be transmitted to Tokyo. ~~and~~ Conversely when they came from Tokyo to Washington, which was our high priority circuit, they'd come by landline from ~~Presidio~~ the Presidio into Washington. Well Earl Cooke, Lt ~~Earl Cooke~~ Earle Cook, in those days, would every morning on his way to work come by the cable company up in Washington and pick up -- well, they had a little dark room -- had a little room ~~upstairs~~ up there with a camera in it, and ~~he would take all the Japanese messages that~~ he would be given all the Japanese messages that had been filed or received ~~that day~~ in the 24 hours preceding. He would go into this little room, photograph them with this little Kodak camera that he had set up there ~~in~~ and the light stand and then bring the exposed film down to a dark room that we had set up in the Signal Intelligence Service, ~~and~~ We'd develop the film and print up the copies immediately ~~and~~ you see and this was a matter of 30 or 40 minutes processing time because we sort of rushed the processing, ~~and~~ We could in those cases, and I've seen this happen many times, we ~~were~~ had the message out and the translation in G2 and the Japs were still servicing the thing to make sure it had gotten through to Tokyo yourself. We had the text of a lot of these messages,

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

and in any case we wanted to I'm sure, we could have beaten the Japs in processing. This is true of the 14-part message because we had that text as it came in typed up and delivered while the Japanese was sitting there still poking out one finger at this typewriter trying to produce that same copy that Nomura and his sidekick needed for Hull. Kurusu, Perusu. (Move to separate line and type a "Q" in the left margin above period in place of "Q".) That's correct. It didn't begin with an "S." Now, as you can see in a as you can probably feel from what I've said in the few months preceding Pearl Harbor, the problems of collaboration had almost totally disappeared between the two services and they had developed a very good modus vivendi between them so that there was progress instead of hinderance, and I think its important to note this because as we look forward down into the post-war years this was one of the strongest arguments the Navy could offer in its presentation of its case for continued separation of the two activities. Now during the war years collaboration problems were not didn't offer much of a hinderance to the efforts with the exception lets say of the weather problem where the Navy felt a strong responsibility that they had to satisfy the naval weather requirements and that they could not rely-- this was a service requirement and this -- You know the counterpart responsibility principle was applied strictly to this in the Navy. Outside of that of course the Army couldn't accept this because our planes fly the same weather that ships sail in and we just couldn't seem to get this across to the Navy, and if we did they weren't in a position to accept it. Outside of this and maybe a couple of other little problems, collaboration was magnificent between them. There was some jealousy which seemed to be

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

generated and I think this was more personal thing. It depended on the individual ~~more~~ rather than the service ~~of~~ as to who could get along better with the British, but Red ~~Cordaman~~ Corderman I think kept the Army pretty much in line, and Smedberg, Capt Smedberg later Admiral Smedberg of the Navy, would not tolerate any nonsense, ~~and~~ so the two chief parties, the army technicans and the navy technicians of GCHQ had no problems that weren't immediately solved by the effective policies laid down by ~~Cordaman~~ Corderman and Smedberg. But it's interesting to note they had to lay down these policies because it seemed to be a sort of a spontaneous thing that the service competitive spirit would tend to go up if you didn't keep it under control, and the fact that they did have to exercise control over it, as I saw it, sort of says that it could've happened if it ~~wasn't~~ hadn't been watched. Well, now things went along ~~swimingly~~ swimmingly, if I can use that term, until the end of the war and then we were confronted on both sides with this kind of a situation. Both the Army and the Navy knew that they couldn't maintain the enormous work forces that had been accumulated during the war in this cryptologic business. So there was going to be a cutback, both in personnel and funds. Another very, very crucial point had to be decided. Early on in ~~WWI~~ World War I the Navy decided that they could not afford to work on any diplomatic system whatsoever; and They therefore announced to the Army that they were dropping all diplomatic work.

Q: (Vnice) WWI or WWII?

A: WWII. This was early in WWII--they announced they were dropping all diplomatic work. ~~They had done this, and~~ They had a little bit on Spanish, ~~They had~~ and a little bit on Italian ~~just a~~ that's a more token effort. The Army had done most of the work on Floradora system. This was Kullback's

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

German outfit. Abe and his people had done some work on the Italian systems, and the Navy had had a token effort and had a small force. They were having pretty good luck on the Italian as I recollect but not much luck on the German. It was a little bit too much of a problem and the load that they, I see, there was a lot of German naval intercept and they just had a lot to work on, but it was a kind of dry well they were pumping at that time because they didn't know enough of about German cryptography. They of course learned from the British about the German Enigma and that gave them a better opportunity to produce intelligence. Now when the Navy made this decision early on in World War II to drop the diplomatic effort, of course the Army was confronted with a corollary problem. Do we, in the Army, concentrate on the military, or do we carry on for both the Army and Navy -- carry on this work? Well I remember that one, General Carter Clarke strongly believed that you would get useful military information out of what the diplomats were saying, and he gave us no choice but to continue and went out and worked very hard to get the authority and the funds and the space and whatever other facilities we needed to continue this work on the diplomatic materials. I can't help but feel like Clarke was a great deal wiser maybe than his counterpart in the Navy. Because the Navy suddenly found itself in a -- I would say, stranded position at the end of World War II because they had no continuity, they had no work force or anybody trained in dealing with let's say the Hagelin ciphers, with the Floradora type of German codes, and the -- they didn't really appreciate the magnificent capabilities which had been developed for dealing

with key generation systems as exemplified in the German one-time pad system you see. We had developed in the Army ~~to~~ the German section had developed in the Army a technique for going behind the text and finding out how the key was generated by the Germans to produce what they call their one-time pads, and in effect the solution to the one-time pad system was not the solution of the one-time system itself but a solution of the machine that generated the one-time system. And this was a sort of window into the wilderness that had never been opened before, and I am being critical now of the Navy for its lack of foresight in developing the broad base of cryptanalytic competence that it obviously would need in the years, hopefully peaceful years -- ~~that~~ which followed World War II. Well this problem that the Navy was confronted with was also translated into a problem the Army had. Could the Army afford to carry on as big an operation ~~and~~ in its attack on the diplomatic systems as it had been able to support during the war years? And the answer was, "It might but it was most doubtful if they could do the full job that was needed. This was because inevitably the funds could be cut back and so we'd be drawn into the situation without the motivation we had before the war to read the Japanese and German stuff because the war was over and at that time we didn't really recognize the problem we had with Russia." I'll talk about that a little later. I might mention right now with reference to the Russian problem that when ~~Gen~~ Truman and Bevin and Churchill sat down at Potsdam and we'd known about the message in which the Japanese foreign office had

directed the Ambassador, I believe was Sato in Moscow, to get the Russians to intercede with the Allies for a dishonorable peace. The only caveat being that the integrity of the Imperial household would be maintained and when that did not surface at these conferences, I think some of us in Washington saw the handwriting on the wall. I know I discussed with G2, and we discussed it among ourselves that the next big problem is going to be the Russian problem. We had some effort that had been started on it. Clarke was a good man to have in the intelligence business in our line of command because he didn't trust any nation. He just said "Look they're your friends today and they're enemies tomorrow, and when they're on your side find out as much as you can about them because you can't when they become your enemy." And he said, "Now lets have a Brazilian section, a Russian section, and have all these things, and lets take advantage of the mistakes they're going to make in war so we'll be ahead of them when the peace comes." And his philosophy was a real good one and I'm glad I recorded it. Now, so we did have an effort on the Russian problem and we did other things, and I think we should have a section on what we did on the Russian as another part of these tapings. Now, lets draw a line and see where we stand at about the time in September of the last year of the war, that would be September 1946. The Navy had no diplomatic problems to sustain its organization. They didn't expect to have much of a navy cryptanalytic problem because major navies had been effectively neutralized. How could it maintain its cryptanalytic continuity, its technical being unless it had some live problems to work on? And where were the problems?

Over at Arlington Hall Station because the Navy had turned over these to the Arlington Hall Station people. Now that's the Navy's, the bind the Navy was in. What was the bind that the Army was in? Everybody was wanting to go home. All the boys in uniform wanted to get out. Some were better cryptanalysts like Art Levinson, Dale Marston, John Seymon, would like to check spelling of his name. Walt Freed. I mention these names because I know them and they were good... Oliver Kirby, and just dozens and dozens and dozens of others who certainly were needed in the peacetime effort, post-war peacetime effort, had businesses they had to go back to. Seymon was a lawyer. Of course some of the people like Dale, and Roy Johnson, and Tom Chittenden to mention just three names had been grabbed right out of at the time of graduation from college they were reservists (you see) and they had never gotten their feet established in the business world, and these were prime candidates. These were the people we ~~were~~ wanted to keep, the Herb Conleys, the Benson Buffhams, I can just name more and more of them. Fresh out of college, right into the Army, right into Arlington Hall Station, well trained, best trained group that you could hope for. You could never duplicate this again in peacetime circumstances and we didn't want to lose these. We wanted a positive thrust and this was Clarke's doctrine. We wanted a positive thrust in the future into -- continue this research in the cryptanalytic work. We'd found out how much it paid off in the development of ECM, and our reinvention and reconstruction of the Purple machine, and the solution of the one-time tape generator that was used for the German one-time pads. These were only three dramatic examples of the other things that we hoped might

TOP SECRET

TOP

be achieved in the post-war years when we didn't have to submit ourselves to the pressures of immediate production of intelligence. The end of the war wiped out some of the cryptanalytic problems, and I think its quite obvious that there was no longer any effort required on three major belligerents, namely Japan, Germany and Italy. These were our three primary targets. The three priorities in the 1930s. Although they had disappeared, other problems had begun to develop. The main two as I recall were the Russian and the [redacted] problem.

EO 3.3b(3)
PL 86-36/50 USC 3605

And of course, there was the very early impulses on the part of the intelligence community to understand what was happening in terms of the Red Chinese movement which had been generated in South China. There was also [redacted] the whole Middle East complex to be continued and in fact reinforced. South America, the Vichy government, and there was a whole variety of rather impressive list of countries that we needed to continue our effort on. From my viewpoint as probably a very selfish viewpoint because in my position in Army the Army effort I was responsible for these during World War II and I was anxious to see the problems which we had kept going throughout the war continued and that maybe we were able to do a better job in producing intelligence from the if I can call them the non-belligerent countries. The Navy had a very justifiable argument that if there was no Japanese navy, no German navy, no Italian navy to work on how could they keep the motivation alive in their cryptanalytic organization because certainly there wasn't enough in the required in the work, on the [redacted] navy, the [redacted] navy to really make much difference

TOP

EO 3.3b(3)
PL 86-36/50 USC 3605

TOP

because these systems were pretty trivial and the navys were not of much importance. I haven't mentioned the Russian navy because quite obvious that was a tremendous problem as well as the [redacted] navy but they needed more than that because to develop the broad understanding of cryptanalysis it was essential. They needed to have reasonable examples of lets say Hagelin machines, Hebern type machines, Enigmas or whatever you might find them. So there was a very strong reason for the Navy to have some kind of a sustaining effort, and a reason for sustaining of the effort would be live problems to work on. There was no countering this argument because it was a solid argument. The Navy also contended and I don't know whether this can be documented or not I never worried about because I don't remember making any such promise myself or anybody else, that when the navy had dumped all the diplomatic work they had been doing in the halls of the Signal Intelligence Service over in the Munitions Building that they had exacted a promise from the Army that the Army would hold them for safe keeping for the war and then returned them at the end of the war. I didn't remember that although it is quoted that I have been party to it. All I remember is, "what in the world am I going to do with all these files that the Navy has left," and some of us must have been real lucky in that we had the wisdom to preserve the files because I think my reaction was to seal them and store them, and thank the Lord because when we started the Pearl Harbor investigation the Navy was real wild to get back to these files and see if they were in tact and they were in tact and I

TOP SECRET

think simply because one sergeant, Johnny Richardson, that I'd given an order to when I became a major, to keep these things properly segregated, and in his responsibility as a storage files officer obeyed the order strictly and it was just sheer luck I think that they didn't get lost in the shuffle of the moves between the Munitions Building and the old Arlington Hall Girls School and "A" Building, and finally they wound up in "B" Building in a little alcove that we'd set aside for historical records. I don't believe this has been noted in history anywhere else but that's about the way it was with reference to the files that became so vital to the Navy when they were defending their position, because the Army itself had to defend its position in terms of the Pearl Harbor inquiry (which was undertaken after the war was over). Now there were a lot of other kind of nasty problems which had to be solved, but I think the real problem which bothered us was how do we sort this mess out here and give the Navy something to sustain its effort so it can so it can honestly go and get the manpower spaces and the budget dollars to keep the proper kind of an effort for the Navy. Well, then the problem began to define itself. If we're going to do a right kind of a job we're going to have something like, and I say it proudly, this old B3, where we had the new cryptanalytic organization would be mainly the diplomatic effort on all the nations of the world which were then coordinated to support the military effort which would need to be developed in case a situation like Pearl Harbor came about again. So you'd have a force in being who was on top of the military systems for the Army and the naval systems for the Navy. And some of

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

EO 3.3b(3)
PL 86-36/50 USC 3605

us who were closer to the B3 operation. I was probably the closest of anybody who was called on to argue how we were going to collaborate after the war. I just couldn't find any justification for breaking up this going this viable organization which was productive and turning out translations regularly and achieving solutions and it seemed to me a disaster if this had to be destroyed. Now this is a very personal viewpoint I had about it because here this was my baby and I just was of course trying to protect it. And I couldn't help but feel that the arguments of the Navy were specious and self-serving because they were not offset by the arguments that I had developed in my own mind for the necessity for preserving this living, breathing, producing organization. I guess this showed through pretty clearly in our meeting where I was called on to testify, and I think when the decision was finally taken that some of the problems would be moved over to the Navy, I recall protesting strongly that if they took the problems they had better take the people and hire the people who had been trained in the problems because we would lose our continuity and I was sure that it would take the Navy a good couple of years to develop the problems with new people to the point that they'd been reached in the Army. And this got through to the intelligence people who were part of the discussions and I scared them. I told them they wouldn't be getting [redacted] messages and those who lived on [redacted] translations got scared that maybe the Navy wouldn't produce them. And [redacted] was another one and [redacted] was another one and Near Eastern was another. And so finally the decision was made, yes if the Navy took a problem they would take a number of people

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

in the section and-- who would be willing to go. For example, the Chinese problem went over to the Navy or a segment of it. Then some of the people would be picked up on Navy rolls who had been previously hired by the Army, and then we would supplement this group by the assignment of some skilled Navy people who were staying on in the post-war days. Well this was, I think, probably the best solution we could arrive at because we also had the problem of a cutback in workforce, ~~and~~ I think we did as well as we could with this kind of solution, probably better than we could if we'd tried any other approach. Well over a period of about six or nine months this problem, which ~~that~~ started out as something to worry about, became a real problem because as we began to move the people over and we could see what was happening, the rest of the workforce, ~~and~~ the low morale, the escape of our ~~most~~ more skilled cryptanalysts from the uniform and in our desire to keep the Kirbys, and the Buffhams, and the Conleys, and the others that I mentioned earlier. We didn't want them to leave. We wanted them to stay so we had to have slots created for them you see in our civilian workforce. The problem just became a tremendous problem and from where I sat and I think quite honestly from where everybody sat there was great doubt that we'd be able to keep enough of these tremendously valuable military convertees on board to satisfy our requirements. My answer to it was single service. Let the Army and the Navy jointly carry on one outfit in one location, and work all these problems together and separately assign naval and army personnel to the unit. Give up either Arlington Hall Station or Naval Communications Annex and just have one because this would be a step forward ~~and~~ in the

HANDLE VIA COMINT CHANNELS ONLY

TOP

achievement of unification and satisfying, at the same time, the services -- and at the same time we would minimize the manpower and budget requirements that we'd have to seek in order to sustain the effort that we'd already developed ~~in~~ and which we certainly shouldn't lose. I think its interesting to note that everybody agreed that we shouldn't lose what we'd achieved. The difference was in whether unification was the answer. Marshall and ~~Caine~~ King had some feelings and ideas about this problem, and there was tensive agreement reached in certain letters between General Marshall and Admiral ~~Caine~~ King that the post-war effort should be designed more or less on the basis of unified effort. I think you will find this ~~corresponds~~ correspondence somewhere in the archives. But there was an exchange of letters and memoranda ~~memorandum~~ between the two in which they both tentatively agreed that the unification consideration should be explored. The judgment was that this would be probably necessary if the work was to be continued. What brought the thing to a head though was the decision was taken, I believe, by Congress, and the bill was passed setting up the Department of Defense with three services, Army, Navy and Air Force. ~~Because~~ All ~~of a sudden~~ at once it became evident to both the Army and Navy that ~~the Air Force was going need~~ there was going to have to be another step in this division, and that some of the problems which the Army had kept and was responsible for, and some of the problems that had been turned over to the Navy would have to be again divided up and the Air Force given some. ~~and~~ This was further complicated by the fact that the Air Force Headquarters was in San Antonio which was hardly within commuting distance.

tentative not tensive?

Tape 4, Side 1 The Air Force in its move to Brooks Field of course generated another problem as it contemplated its organization's headquarters in San Antonio because it was a lot further from Arlington Hall Station and the Naval Communications Annex ~~Brooks Field~~ than it was just across town between the two local stations ~~and~~ the further complication of distance added to the (problem of the) division of the effort ~~were the~~ was a most distressing thing to contemplate. Things got a little bit out of our hands. The responsibility for making this decision and thrashing it out among us was taken away from us by the Secretary Royal who was at that time was Secretary of the Army (and) who had heard about the intentions of the Air Force to set up this third SIGINT effort, ~~and~~ he was already a little bit distressed about the problems that had been reported to him that had arisen between the Army and Navy in trying to divide up the Washington effort. He talked to Mr. Forrestal about this -- ~~Mr.~~ Forrestal being the first Secretary of Defense and considerably Navy oriented because of his naval experience at the secretarial level and as a result of Royal's interests in conserving both money and preserving ... I mean both conserving money and preserving continuity, Forrestal arrived at the solution, ~~and~~ I'm not so sure that this ~~is~~ was the best thing he could have done because he might have made a decision, I guess that's the fault I find with it. He set up a board to study the problem. Well the problem had already been studied by the people who were most knowledgable, ~~and the~~ (This) board simply took it out of the domain of the people who understood the problem and put it into the domain of people who were responsible for making decisions without maybe too much knowledge of what they were

deciding about. So a board was set up and on it were representatives of G2 and Arlington Hall Station, Col Hayes, who was the head of the Army Security Agency at that time, was a proper member of the board; I was a sort of secondary member, (and) The head of the special branch G2 was also a member. These two positions were matched by the analogous positions in the Navy and Air Force. ~~so and~~ Then there was a chairman of the board and I, ~~in~~ at this point in time, cannot identify who was the chairman. The board took its time in getting started. I suspected at the time and I have no reason to believe otherwise today that the Navy and Air Force ~~drug~~ dragged their feet in the hope that time would solve the problem and they wouldn't have to be confronted with ~~the~~ unification. ~~of~~ They just hoped it would go away. But it didn't go away because the pressures and budget manpower kept becoming increasingly evident and some response had to be given to them. ~~and~~ The Air Force was (also) having trouble in getting justification for its budget ~~at~~ for Brooks Field because the problems ~~were~~ was still in an unresolved state. So despite their reluctance to deal with the problem it was forced on all; the Navy and Air Force reluctantly, and happily in terms of the Army because the Army had made up its mind it was for unification. We believed in it. General ~~Boeing~~ Beiling believed in it. ~~Col~~ Carter Clarke believed in it. Hayes believed in it, and those of us who had seen the way Arlington Hall Station had worked also believed in it. ~~and~~ We thought it was an essential thing from the COMSEC viewpoint. So the Army was solid for unification and of course out of agreement with the Navy and Air Force. I don't think the Air Force really knew what it was proposing because the people, and I do this not with the intention of denigrating the membership of the Air Force on the

board but they just didn't have anybody who was knowledgeable. We found it most difficult sometimes to make ourselves understood by the ~~A~~air ~~F~~orce members when we tried to explain a point dealing with the handling of ~~the~~ a technical problem. These discussions of the board resulted in several proposals. I remember every week came ~~it~~ there was a new proposal. ~~that~~ The the ~~A~~ir ~~F~~orce would have a proposal, and the ~~N~~avy would have a proposal. ~~and~~ Then the ~~A~~ir ~~F~~orce and the ~~N~~avy would join their proposals. ~~and then~~ The ~~A~~rmy would come in with a counterproposal, and the whiter the ~~N~~avy-~~A~~ir ~~F~~orce proposals got, the blacker in contrast, ... well the more diversified the ~~N~~avy-~~A~~ir ~~F~~orce proposal became, the more 'unified' the ~~A~~rmy proposal became, if I can do a pun, and so the situation instead of ~~better~~getting ~~ing~~ got worse. I look back with a certain amount of dissatisfaction on my role in these discussions because I remember the first time I was called on, I got up and made an impassioned speech for unification threatening the loss of any continuity that had been developed by the ~~A~~rmy during the war and the thrust of this was that I didn't think the ~~N~~avy and the ~~A~~ir ~~F~~orce could do what the ~~A~~rmy had done. This was the interpretation given to it. It was a very poorly chosen presentation that I ~~did~~ gave but quite honest and from the heart and I would probably do it today if I had to do it over again. As a result of this I became persona non grata to everybody except the ~~A~~rmy who was on this committee ~~and~~ Pretty soon the ~~N~~avy and ~~A~~ir ~~F~~orce proposed that I be replaced by somebody else. Hayes declined to replace me, but said I would not sit at the table any longer but I would certainly be there in support of you. Well this was a half victory for both of us and in counsel with ~~Boeing~~ Bolling and Clarke and Hayes I was encouraged to speak my ~~peace~~ piece

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

TOP SECRET

fully and clearly and as emotionally as I saw fit, and if they couldn't pick up the pieces it was just too bad. They didn't discourage me at all and I'm grateful for that, but I think that I might have used better judgment in presenting my arguments. Actually most of the Army's staff work on this was done in the intelligence division which had come into being ~~at the~~ as we reorganized the war time effort to the upcoming peace time effort, ~~and~~ I think this was a healthy thing we did in the Army, and it does have a bearing on the unification problem, so I might describe how the Army concept of dealing with the cryptologic problem was exemplified. It was evident that we had to have the best specialist we could find in COMSEC, ~~and~~ In our concept COMSEC was more important then COMINT and why?

EO 3.3b(1)
OGA

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

EO 3.3b(1)
OGA

Well there was a little bit of that in their attitude ~~but~~ that we had at whatever cost to protect our own communications, and COMINT while interesting from an intelligence viewpoint was important to a large degree because it enabled us to have a better understanding of the weakness of the cryptographic systems which then we could fold over into the improvement of our own systems. Now this was a little bit of the Arlington Hall view so we made sure that our COMSEC organization was properly staffed. Then we realized that there was a great quantity of effort that had to be expended ~~to~~ toward the production of intelligence and exploitation of intercepted messages. ~~and~~ So this became the intelligence branch of Arlington Hall Station. So we had the two poles COMSEC and COMINT. Then there ~~were~~ war a great and most important area of the development of new techniques and equipment computers we now realize were important. We kind of got stopped on our investigations into computer ~~during~~ usage in satisfying the needs of the wartime effort. So one of the domains that had to be fully explored was what could we do in the development of computers that would enable us better to solve foreign systems and better to evaluate our own systems, ~~and~~ We saw in the analogs of the Enigma that the British call the Bombe and our Madam X out at Arlington Hall Station. We looked on these as only an interim solution in a feeble effort in the direction of more sophisticated, real, high-speed electronic devices. Grant its a dream, but the dream was there and the vision was there, ~~and~~ We looked on this research and development component that we had visualized as administering the new

~~TOP SECRET~~

~~word~~ work in development of high speed devices, better means of intercept, and whatever was needed in support of ~~either the COMSEC or~~ both the COMSEC and COMINT effort. (It) would be developed right there and we would have the best experts we could find turning ~~our~~ their brains on to the solutions of the problems which had been generated by the COMSEC and the COMINT efforts. Also we visualized this central function as a place where the COMSEC and the COMINT would be married. We could see from our wartime experience that people who ~~would be~~ were involved in the day-to-day production of COMSEC materials were so preoccupied that they might not have the time to do the ~~corporate~~ forward thinking and learn about the cryptanalytic techniques that were important. Conversely the people who were dealing with the day-to-day production of intelligence, the exploitation of intercept, would be so preoccupied with that they would let slide the marrying of the COMSEC/COMINT interests ~~to~~ necessary for ~~the~~ ~~improvement of the~~ development of new and improved systems. ~~and~~ We saw (that) the concept of ~~the~~ a research and development (effort) sitting between the COMSEC and the COMINT, where the work was done for both efforts, would be a better administrative arrangement than having two separate research + development organizations, one in support of COMSEC and one in support of COMINT. So the three legged, the triumvirate concept is the one we bought. ~~and~~ I think this is important to note because this was the theory behind the Army's proposal for unification that it developed. Now in contrast to the Army's concept that the Army had proposed, the Navy and Air Force had a variety of concepts. I'm not sure that the Air Force really ever crystallized in its own thinking what kind of an organization it wanted to set up. I think they were, by the by virtue of their association with the Navy

~~TOP SECRET MAGIC WAR COMINT CHANNELS ONLY~~
TOP SECRET

as being opposed to unification, ~~were into~~ willing to accept~~ing~~ the Navy solution to this future problem, and the Navy in its efforts to overcome the Army's solid position on unification tried to, as I mentioned earlier, a variety of suggestions. I think one of them is worthy of note, and I will give a little bit of the background why they latched on to this and pressed it to the degree they did. We found that toward the end of the war there were a variety of things that just weren't getting coordinated, ~~and~~ So I believe Billy Friedman had proposed the establishment of some kind of a coordinating committee which insured ~~that~~ the full and free flow of technical information between the cryptanalysts of the Army (Arlington Hall Station) and the Navy cryptanalysts. I don't think this was really needed but it did serve to bring out into the open some of the problems that had been festering between the organizations... Little problems which if you didn't watch and solve could become big problems. ~~And~~ There were a few of these, the weather problem I mentioned earlier ~~was only~~ was probably the biggest one, and there were other little problems like dealing with plaintext, division of intercept, keeping of records, what to do about, well, one of the important things that developed was how do you record technical successes? How do you perpetuate and pass on knowledge? For example, if you solve a new Japanese system, how do you insure that knowledge gets to other people who could use it? ~~And~~ These were the kind of problems that we had tried to achieve some ~~kind~~ sort of solution for in the Army and ~~was~~ we'd set up under a fellow by the name of Maloney and Miss Margaret Hancock, a little bit of a cryptologic

(delete comma)

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

TOP SECRET

storehouse of information. ~~and we had matched~~ The Navy had matched this so we were making some effort to get this exchange going and it was pretty successful. But some of the nastier problems like the weather problem just didnt get resolved at this level and had to be dealt with at a higher echelon. Actually I don't think the higher echelon really knew what to do about these problems so they were quite glad to have Friedman's proposal to set up a coordinating committee accepted and we called this the Technical Exchange Committee to start with, I believe we called it "TEC" and some of us punned TICTACTOE you see to boot. It worked after a fashion and we supported it and did participate in it, but I think the back-of-the-scenes collaboration continued to satisfy our major hungers much better than this committee. Well pretty soon this committee ~~itself~~ got itself seized by trying to solve the unification problem. And then it became apparent that this might be a useful gimmick if the Navy and Air Force accepted this as a solution because the committee I think itself wanted to perpetuate itself, wanted to become more responsible. Then we also had another problem and that was the liaison problem with the British you see. What were we going to do with the British after the war became a very important thing in ~~the~~ both the Army and Navy ~~because~~ Do we continue this collaboration in peacetime era, or is it better to stop it for security reasons ~~or~~ and go back to our isolationist position in terms of technical collaboration and just what do we do? Well most of us who had worked closely with the British kind of felt like they were going to suffer from the same kind of problems that we did. ~~and~~ Even though they were obviously going to have much less money than the American

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

community to invest in cryptanalytic work they also had a long history of successfully carrying on this kind of effort even with a minimum of support, financial and manpower. And we thought it would be useful even though they might be smaller than either the Army or Navy ~~even~~ if we did have ~~to~~ two or even if we had three. It was to our advantage to continue this because we were aware at that time that the Russian and Chinese problems, the communist problem if you will, was the big problem ahead of us. Now there was then a structure devised and this sort of grew out of the kind of problems generated by the collaboration with the British in which among other things there was an ILG set up. This was the liaison group.

EO 3.3b(1)
OGA

[redacted] Then there was another group in which a COMSEC coordination kind of thing was set up and then there was a cryptanalytic exchange group. I was deeply involved in the cryptanalytic because of my position as the head of the intelligence division so I was pretty well involved in this, ~~and~~ I was also deeply interested in what [redacted] was doing because he was getting in my hair with his liaison group, ~~because~~ I didn't want to filter the technical exchange between the cryptanalyst ~~and~~ in the intelligence division and the cryptanalyst in the Navy and the cryptanalyst in Britain through a bunch of unknowledgeable people that [redacted] represented ~~because~~ Since he had never been in the COMINT business as a practicing cryptanalyst. Now these I mention not as great problems but the kind of problems that just kept coming

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

up day after day, and ~~you didnt know what to do with and nobody wanted to get a good answer.~~ Well, while everybody wanted to get a good answer to them, nobody was willing to accept the other guy's solution. ~~and~~ This is no way to be successful in the COMINT/COMSEC business. Now this technical liaison group, the coordinating group, then all of a sudden got itself involved in a lot of these things and looked like it might be a good way ~~around~~ to avoid the problems that were being otherwise generated. So from this came the basic proposal that the evils, the post-war evils, be solved by some kind of a coordination mechanism. ~~and~~ Finally the one which came out involved not only the technical exchange, which had grown up from the requirements from the Army and Navy group, but ~~and~~ finally got over into the intelligence requirements. ~~and~~ Then it became known as the Intelligence, the CIB, Communications Intelligence Board. So the CIB ~~STANCIB~~ and then we got such things as the Army/Navy Intelligence Organization. ~~and~~ Then State got into it and it became STANCIB, and I don't know what happened when the Air Force came in... I kind of forgotten, but these kind of things grew up sort of as antidotes to the poison of lack of unification. I'm sure these discussions are the problems are well documented ~~and~~ in the deliberations of this committee. Incidentally I believe it was known as the Stone Board because of Admiral Earl E. Stone who was the head of it, and if you want to dig into the Archives and pick out the Stone Board reports you'll get the whole story much better than I can recall it.

Q: Were they doing any Stonewalling?

A: Not the way Nixon did.

Now lets kind of get down to how this mess was resolved. Finally the

HANDLE VIA COMINT CHANNELS ONLY

Stone Board agreed that it would turn in a report. The Navy and Air Force had stonewalledly opposed the split report. The Army had just as stonwalledly declined to send in a unamimous report or declined to send in a compromise report in which only the things that were agreed upon would be reported on, and the rest of them would be unresolved. So the Army wrote a minority report and put the stamp of final approval on it and said this is going up regardless of what the Board puts up, and you Army and you Navy and you Air Force get together and write whatever kind of report you want and call it whatever you want to but this is the Army answer to the problem that we've been charged with and that the Stone Board is responsible for, and Alex Bolling authenticated this stand and that's where we stopped. Well this brought the whole doggone series of dialogues to an end. From the back rooms of Arlington Hall Station, Naval Communications Annex, and the Pentagon rooms where the Air Force had its headquarters, It just all jelled into a split report with what they called they called the minority report which was the Army solution, and the majority report or the Board report which was the joint Navy/Air Force. Well this went up to Forrestal's office with Stone's letter saying that the committee had performed its function and we thought there was nothing else they could do. I don't know whether he dissolved the committee or not, but anyhow things got awful quiet for a while so far as the Stone Board was concerned. But things got worse so far as what we were trying to do because the Air Force came in and insisted

TOP SECRET

they have some of the problems, you see, with ~~that~~ authority and before the Secretary of Defense had solved the problem, ~~and~~ I think one (more) interesting thing happened that I need to tape, because it might otherwise be lost, was (that) in this interim [the FBI began to raise its voice and say it wanted a cryptanalytic organization. ~~And~~ I think it was within this time frame, and I believe ~~the~~ my friend Ham Wright really got boxed in on this one because ~~his interpretations of his instructions~~ when the Bureau representatives came down to see what kind of effort they could undertake he interpreted the instructions that if they found something they could usefully undertake that he would turn over the responsibility to the Bureau for this cryptanalytic effort. Well, unfortunately for Hamm he chose and did in fact start to turn over one or two or three problems ~~that~~ (which) the Navy had taken over from the Army, ~~and~~ he couldn't have pulled a bigger booboo if he'd sat down and planned it for two years because what did this do? It just proved the Army's point that you couldn't trust the Navy and if you turned these problems (over) the first thing you know they'd just be shuffled around just like a new deal every year or two, you see. The Bureau wanted the problem, so the Navy gave it to them.] There was a second (slip) in the loss of continuity and this was a beautiful one. I remember being real angry about this, not at Hamm but at the stupidity of the act because it was (just) complete contradiction of everything that I had believed in and I wanted to see happen. So Dink Hayes who was the head of Arlington Hall Station at that time was ~~a~~ the CJO or Coordinator of Joint Operations and when I reported this transfer to Hayes, Hayes was as angry as I was and he wasn't angry because I was (angry)

FBI

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

~~TOP SECRET~~

He was angry because he believed this as violently I did. ~~And he~~ called up Admiral Stone, and he ordered Stone as CJO not to permit these problems to be turned to the Navy. ~~and~~ Then there was a hell of a big conference which I attended in Hayes' office the next day in which Stone and Wenger and Hamm Wright -- and poor Hamm sat there like a dog with his tail between his legs being beaten by both Hayes who did everything but call him stupid, but that was quite clear that Hayes thought this was a terribly stupid thing, and Stone and Wenger, on their part, denying any responsibility for this; so poor old Hamm took the beating. But I think I think this shook Stone up. I think he began to understand what we were trying to -- the point we were trying to make. ~~and~~ With this sort of in the background I think the Navy was a little bit weaker in its pressure than it was before. Now I've told this story of the turnover -- the problems of the Bureau sort of out of context. I don't know whether it fits into the Stone Board report or not because I'm sure that it would not show up in these things but this is the kind of thing that was happening and had to be resolved. ~~and~~ Until the unification question had been settled this is an example of the kind of thing that was going to keep coming up time after time again and which there would never be any good answer for because there was no authority for that except the somewhat questionable authority of the CJO, ~~and~~ If I'd had been Stone I'd called Dink Hayes and said "Buddy, you got no authority over me. I got the problems. I can do with them as I, Earl Stone please. I am an Admiral in the Navy and I rank you Colonel." and that's the way that I would have handled it.

FBI

~~TOP SECRET~~

But I don't think I would have made that judgment to start with. But this was a very fluid, flexible, nonsensical situation and most distressing to those of us who were at the crox, who were at the meeting point of at the crossroads where the problems met ~~because~~ because, you see, there were just so many problems coming in from every ~~where~~ road that we just couldn't deal with them. ~~and~~ We couldn't do our work, because there was no way of solving these problems. ~~because~~ They just stayed and ~~natted~~ nattered and ~~natted~~ nattered and ~~natted~~ nattered and laid on our back. Now I'm a little emotional about this because of the terrible way to do the things that needed to be done because there was the cutbacks, we had to cutback the forces; we had to figure out who we needed to keep in the business; what to do about the Kirbys, and Buffhams, and Conleys; what to do about the other kinds of things that were just with us and needed immediate decision, and then there were budget cuts. How do we get money for this project? What do we do here? How do we get better intercept for the Russian problem? And all these things were just raising hell all over the lot and thats the chaos that we found. Well it was quiet as far as the Stone Board was concerned but it wasn't quiet so far as the problem solving was concerned; It just got worse. ~~and~~ Then, unfortunately, something happened to Mr. Forrestal. He committed suicide. I've got to go back and correct part of this tape. I said Johnson. It was Kenneth Royal. Did I mention Royal who was - then I was correct. But Louis Johnson then became Secretary of Defense and took over after Forrestal's suicide, ~~and~~ He got General Joe McNarney to come and work half-time in his office

TOP

and McNarney's problem his assignment was to go through the unfinished business left by Mr. Forestal, ~~and~~ In his search of these files that Forestal had left, McNarney found this split report and he took it away and he studied ~~and~~ Mr. Johnson had emphasized his interest in doing whatever they could possibly do to satisfy Mr. Truman's charge to him that in the creation of the three services the new Secretary of Defense would emphasize the principles of efficiency and economy in developing the new organization. This was sort of the watchword of the instructions conveyed by Johnson to General McNarney, ~~and~~ In reading the Army report, for some lucky reason, we had written as two of the major advantages that this would be more efficient and more economical, and they stood out just like red letters in the new testament. How lucky can you get? You know one of the mottos of a cryptanalyst is, "It's lot better to be lucky than smart." So this stuck in McNarney's mind and he went in to see Mr. Johnson, ~~and~~ He pointed ~~it~~ out these particular aspects of the report, namely that the Army could claim economy and efficiency but the Air Force/~~and~~ Navy solution did not claim it. Mr. Johnson made a simple decision. He said "Well, Mr. Truman has told me, The President has told me that I got to do some efficiency and economy, and if the Army thinks this is efficient and economical, we'll do it," and what do we do?" McNarney said, "why don't we talk it over with Mr. Truman, The President? Let him know what you're doing. Not only will this show that you're working hard on this, but it will (also) be evident that you're getting something done in this direction." ~~and~~ So Truman, when he heard that the Army said that it would be more economical and efficient, he said, "That's for

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

us boys, I'll initial it, and Then it happened. It happened. It came in the room like a thief in the night. Nobody knew that McNarney and Johnson were going up and dealing with this problem with Truman, because everybody thought it got lost in Forestals papers, and of course the Navy and Air Force were real happy because they had bought a lot more time. Well we were very much shocked when Bolling called Clark, Hayes and myself over to his office and told us what had happened. Then Bolling charged Clarke with the responsibility for drafting the implementing order, and Also charged Clarke with the responsibility for doing whatever else needed to be done on the part of the Army to satisfy the requirements of this decision by Secretary of Defense. Well about that time we saw the draft of the letter approving this which McNarney had drafted for Johnson's signature. I think its in the Stone Board file. Its a beautiful, terse, two-paragraph letter, The intent of which is vividly clear. You will consolidate. And it doesn't say how you do it, but it sets parameters for consolidation to limited those measures which insure efficiency and economy and that these will be the guiding principles under the consolidation. Obviously the next step after the Secretary of Defense had made the decision for unification was the creation of some kind of organization which would in fact unify the Army, Navy and Air Force efforts. A blueprint had been presented by the Army for a so-called Armed Forces Security Agency and McNarney looked upon this as probably being the best that could be done at that point in time, so it was inevitable that an Armed Forces Security Agency would be formed because there wasn't any kind of a better thing to be

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

adopted. The general organization was along the lines of a central, three-pronged COMSEC/COMINT/R&D structure with such things as Administration, Training and Liaison in a staff level. These were the important things. There were other things. Policy Staff had to be provided for. And then there had to be some provision made for what somebody erroneously called the residual services which would remain with the Army, Navy and Air Force because, even though we wanted to consolidate the cryptanalytic organizations, we felt that the intercept should not be consolidated and that the services should be held tightly responsible for the production of intercept both for the counterpart responsibilities and for the consolidated responsibilities in which mainly in peacetime would be developed around effort on the diplomatic problems and whatever active military problems could be dealt with at the consolidated level. We rather insisted in the Army report and this was followed that the main thrust of the effort on the military systems would be conducted in proximity to the diplomatic systems because in the case of some of the problems it was evident the cryptologic principles the cryptographic principles were generally followed through-- the same principles are generally followed throughout the services. Well, a good example was the German because the German army and air and navy all used the Enigma device with slight modifications, but the basic principles of the Bombe which was used for solving them applied all across, and only minor modifications, if you will, had to be made to the Bombe for it to effectively operate on traffic of any service. We had a lot of problems. The problems didn't just go away right quick overnight because of the consolidation. Such things

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

as moving the Navy SIGINT effort over ~~at~~ to the Arlington Hall Station, and the Army COMSEC effort over ~~at~~ to the Naval Security Station, where the location of the Director's office was going to be, where the location of the staff components, training, whatever else was needed, what kind of an organization would take place in the services for the three cryptologic services and how these would be resolved. But this all had to be done within a sort of sudden timeframe because once the Secretary of Defense gives an order, it gets implemented or it did in those days, I hope it still does, if it's a good order. Now my role in this thing I might talk about a little bit because I was directly involved as being the head of the intelligence division of the Army Security Agency. I was directly involved with making sure that the people in the Army Security Agency fitted into the new organization. ~~Reggie~~ Rosie OSY Mason, Capt Mason, was selected as the head of this new AFSA Intelligence Division. I forget what its name was. I think it was AFSA 02 because we went to sort of cover names in those days. So ~~Reggie~~ Rosie OSY was the head of AFSA 02 because I was a civilian, I was and the senior member in the Army, it didn't make any difference whether you were civilian or military you could have command responsibilities but seemed like with some concept which the Navy and Air Force had the command positions would be held by ~~the~~ a regular Army, Navy or Air Force officer rather than a civilian. I think ~~Reggie~~ OSY was a good choice, and I ~~also think~~ ~~Reggie~~ Rosie OSY was named as AFSA 02. ~~and~~ I didn't at all mind being ~~his~~ as the AFSA 02A I believe ~~as~~ I was called because I was responsible for

insuring technical progress was maintained within the organization. That was my job responsibility but my actual duties were to make sure the Army and Navy outfit so far as the Army members were concerned, were organized so they got along and there were no personality conflicts and there was fairness, fair treatment given to all concerned. We had a couple of little problems that came up, more personality problems because ~~Reggie~~ and I got along so well together, these problems were resolved just as they began to appear. We just did not tolerate any maliciousness or any interservice fighting. If we found a clique of Army lovers fighting a clique of Navy lovers, we'd beat the heads of both together and nobody came out with honor, and pretty soon the word got around and the ~~algamation~~ original formation went along pretty smoothly. Of course, there was always this undercurrent of "he's Army - he's Navy" and that kept going on and still probably goes on. I think we can avoid a little bit of it, I could name a couple I saw just as I walked out the door after my retirement ceremoney but I won't, ~~and~~ I don't think we'll ever get away from that as long as there is some substantial residue of the two services and I don't know if its a bad idea for it to be there because as I look back and this is one of the strong Navy points opposed in opposition to consolidation that the competitive spirit is a useful thing to have happen ~~and~~ if you want~~ed~~ to develop a good cryptanalytic organization except for some reason I ~~was~~ always argued that it ~~was~~ better to fight the enemy than it is your friend. In due course the organization started producing again. ~~It~~ There was a ~~rather~~ lot of feeling expressed, particularly on the part of the people who originally worked for the Army, then when the problems were transferred to the Navy they were picked up on Navy roles and now they were shuttled back from Nebraska

Avenue and had to move back over to Arlington Hall Station, ~~and~~ This seemed to be a most unfair thing, but we made arrangements whereby they could be given other jobs in other parts of the organization, ~~and~~ granted this wasn't a very efficient way of dealing with the problem, but it was a humane way of dealing with the problem and finally these difficulties began to disappear and AFSA settled down to getting on with its work. Of course the ~~foundation~~ formation of AFSA was only the beginning of another series of adjustments that had to be made in the organizational structure that dealt with intelligence and COMINT and security, that's COMSEC security. For example, the term Armed Forces Security Agency, which had sort of been proposed by McNarney as the appellation of the new organization, had the connotation that it dealt only with the problems of the Armed Forces, the Army, the Navy and the Air Force, and almost

EO 3.3b(1)
OGA

to find out the responsibility of AFSA ~~on~~ for doing anything on the diplomatic traffic, clandestine traffic which was required by CIA, and the internal U.S. traffic which would be the responsibility of the FBI. A committee was formed, an advisory committee if you will, to the Director of AFSA which was an outgrowth of this extensive concept that had been developed earlier, and the question was whether CIA, the newly organized Central Intelligence Agency, which had no roots at all in the COMINT production business, and whose activity ~~at~~ up to that point in time

EO 3.3b(1)
OGA

Certainly there was no question in the minds of anybody that it CIA was to do the kind of job that it had been charged with that it would have to have the output, but it was also quite evident at that point in time that you

couldn't intelligently run a COMINT producing outfit and I'm talking only about COMINT in ~~that~~ this context without some sort of a feedback of requirements from the intelligence consumers, ~~and~~ This lead to a series of discussions and finally the problem was resolved somewhat along these lines ~~and~~ that the name AFSA, Armed Forces Security Agency, was changed to National Security Agency because the connotation of National Security Agency embraced the requirements of the other elements of the government who had an interest over and above the three military services. The line of command was also changed from a lower echelon in the Department of Defense I forget now but I think it was the Chairman of the Joint Chiefs of Staff (at any rate) at that level that the AFSA reported to and the new National Security Agency was elevated to the position of reporting directly to the Secretary of Defense. In due course a National Security Intelligence Directive known as NSCIDs, NSCID 9 as I recall specifically dealt with the organization and the responsibilities of the National Security Agency in its relationship with the so-called consumer agencies as well as the military agencies. This tended to resolve a lot of the nattering problems because it gave us a sort of code of laws that could be applied in the ~~judication~~ adjudication of any conflict of responsibilities, and laid out pretty clearly the role of the cryptologic services as well as AFSA and the consumer agencies, and I think most happily indicated that all cryptanalytic work would be done within the National Security Agency cryptanalytic in the sense of the COMINT production activity and the exploitation. But it took

away from NSA the responsibility for evaluation and reporting and left these functions with the so-called consumer agencies. Now history has sort of developed another modus vivendi so far as this reporting is concerned but I think these are proper developments subsequent to the resolution of the basic conflicts in responsibility which were ~~pressed~~ present before NSA was called NSA and the NSCID was written. I think it is important to note because its effect isn't normally observed ~~in~~ within the working components of NSA something else that the NSCID 9 provided for and that was a special committee of USIB called a Special Committee and it was comprised of the Secretary of State, Secretary of Defense and involved the Director of NSA. So this Special Committee made the decisions about the real difficult decisions, ~~it~~ and was supposed to resolve the real difficult decisions. I know of only one instance they dealt with that amounted to anything, so when the NSCID 5 replaced the NSCID 9, and incidentally, I don't remember the full details of this one problem they had, but it was not much really not too well resolved by the Special Committee because they just didn't have the understanding of the problem that was necessary. It wasn't a single affirmative or negative answer. It was a ~~continuous~~ continuing review, and you just don't impose on the Secretary of State and the Secretary of Defense this continued responsibility of dealing with the same problem over and over again as it evolves. So when NSCID 5 replaced NSCID 9, and I got this word from Allen Dulles himself, it would be useless for us to perpetuate this special committee but the full responsibilities for the policy making apparatus which directed developed the policy considerations followed by the Secretary of Defense in his administration of the National Security Agency would be laid down by the USIB committee. This seemed to work out alright

because I followed the Committee pretty closely both before I went to CIA and then I probably attended ... well I attended every meeting of USIB that was possible for me to attend when I worked for Dulles and I saw this structure evolve so that it did fill the gap that was expected of the Special Committee. Now I think another very important development took place when NSCID 5 was written because there used to be two committees, USCIB and USIB. The US Intelligence Board or committee, I don't remember whether it was board or committee, and then the US Communications Intelligence Board. Now under the NSCID 5 concept, as I recall it, the two boards were joined and they dealt with the total intelligence policy rather than ~~with~~ separating it out and having the regular intelligence of the non-COMINT dealt with by the one board and the COMINT by another.

Tape 5, Side 1 The ECM as useful as it was and as wonderful as it was was not the total answer to the code machine requirements or the cipher machine requirements of both the Army and the Navy. The Army had a more pressing requirement for another type of device. Namely one which would automatically encipher teletype signals so that you could get automatic on-line operation of the cipher machine which ~~is~~ was entirely feasible at that time in terms of the state-of-the-art, except that the cipher machine ~~that~~ which would efficiently work ~~would be~~ with the IT&T and other automatic teletype equipment just hadn't been developed and linked in with the transmitting installation. General Stoner and his staff, the Army Communications people, early identified this missing piece of their

~~TOP SECRET~~

communications gear and brought pressure on Signals Intelligence Service either to develop a cipher machine which would securely disguise the teletype signals, or work out some way whereby a device could be constructed by a contractor... Hopefully IT&T who had done such a magnificent job on the manufacture of the ECM or the SIGABA. At that time I was pretty busy with the organization of the I'll call it the B3 cryptanalytic unit which was essentially everything but the Jap, German and Italian military organization, and later did embrace the Japanese military attache and certain associated military systems, ~~and~~ This requirement was placed on us initially just before we made the move to Arlington Hall Station. I think it was along about March or April certainly no later than May as I recall. ~~I was been~~ We were about to move to Arlington Hall Station. I was spending considerable time working between the Munitions Building which we were leaving and going over and seeing how the small units -- some of them were in the Pentagon, some of them were in the Headquarters Building, Arlington Hall Station were doing. So one day when I came back from Arlington Hall Station Friedman sent for me and asked me to come to his office, ~~and~~ He said, "I would like for you Frank to look over and witness the recording of an invention that I have produced. This is to satisfy the requirement for this automatic teletype enciphering device that Army Communications people want, and we need some kind of circuitry which can be incorporated into a piece of gear that can be used with the teletype tape transmitters and which can be operated directly on the line so that you've got real time encipherment of the signal and real time deciphering of the signal. Well I looked over his

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

TOP SECRET

diagram and it was a pretty clever idea except it had certain circuits in it ~~which~~ that just wouldn't permit the thing to operate. ~~The~~ This was a disappointment to Friedman when he found out about it. I could go into this detail because I think it shows just how these things come into being, ~~and~~ he was real shook up because he said, "Well, we've got to have something that will satisfy this requirement because we're going to ... they wanted to set up some new circuits between the US and North Africa and this is an urgent requirement. It's going to be talking about the convoy sailings; they're going to be talking about shipment manifest, and a lot of vital information which, if the Germans knew about it, could be disastrous to the plans for North Africa." Well there was no arguing with this so we sat there and batted the idea around for a while and I had been working between the time that the M1 ... that the ECM had been produced and Pearl Harbor--sort of inbetween Japanese chores, I had been working on a variety of circuits, printing mechanism for all sorts of enciphering concepts, just for my own amusement to see what could come out, ~~and~~ I recall that one of the ideas that I distilled out of this had to do with teletype encipherment, ~~and~~ my curiosity in this particular instance when I'd done the thinking about the idea was could we use ~~the~~ a cipher wheel to generate a key or a batch of cipher wheels to generate a key which then could be used as a five-baud encipherment. And it came out pretty obvious as I looked at it. All that was needed was to take the control rotors in the ECM, disassociate them from the substitution maze rotors, and feed the circuitry from the end plate which normally would go to the solenoid controls on the five substitution wheels and just feed these circuits into a set of five relays which would then

[illegible] CHANNELS ONLY

TOP SECRET

TOP SECRET

operate in the conventional ~~Burnum~~ Vernam mixing pattern. ~~Burnum~~ Vernam is the man who invented the automatic enciphering machine in early 1920s, ~~and~~ It was already well known in the state-of-the-art that you could mix a key signal like a one-time tape with a plain language signal so that you got a fairly good encipherment, automatic and actually instantaneous of the plain language using this principle. So what I was really doing in my proposal that I developed for Friedman was to take the output of the control maze from the ABA and feed it in to take the place of the ~~Burnum~~ Vernam tape impulses in the mixing apparatus that he'd put together for his earlier cipher machines. This wasn't a very remarkable idea by any means but it was new and it hadn't been done before, ~~and~~ It was obvious that the thing would work because we knew enough about the impulses on the control maze on the ABA to have tested it, and we knew enough about the operation of the old ~~Burnum~~ Vernam cipher machine to know that that worked, and it was real easy to imagine that the signals through the cipher wheels would simply replace the tape ~~or~~ of the ~~Burnum~~ Vernam apparatus and we had an automatic cipher machine. Well this delighted Friedman and I was feeling pretty good because it was a chance to do something toward speeding up the cipher program without too much effort on my part. So we developed the idea on paper there at his desk and put it in the form of a proposal, and we both signed it and got witnesses on the thing as an invention within a matter of two-three hours. And then Friedman took it up to Army Communications and the IT&T engineers in due course and when I saw him in a couple of weeks he said I think we've got something that's going to satisfy the requirement. IT&T is real pleased with the

[illegible] COMMUNICATIONS ONLY

TOP SECRET

TOP SECRET

prospects of putting it into hardware and General Stoner is real pleased that we got something that IT&T wants to do and thinks they can do within the time frame that is required of him. Well I guess in peace time, if there hadn't been a war on I'd stayed closer to it, but I kind of lost track of it at that point in time and we moved over to Arlington Hall Station and great droves of people came in and I didn't have much time to get involved with the COMSEC things until I was invited over the see the first model of this some few months later in operation in a small, isolated area. I don't remember whether this was in the Pentagon or Arlington Hall Station or in the Munitions Building, but there it was working and working beautifully and Stoner was delighted. So evidently the COMSEC people and Army Communications people and IT&T thought this was quite adequate for the fast communications requirement and I didn't think much about I didn't worry much about it because I was worried about other things. Now when the device came out into production it was at a very good point in time to establish the first link between Washington and North Africa. The Army Communications people took one radio circuit, a two-way circuit - a teletype circuit, and installed two devices on each end. One of those devices was for enciphering the transmitted signal which went from Washington to North Africa and the other of the devices was to decipher the signal that came from North Africa to Washington. Of course there had to be a encipher/deciphering arrangement on each end because you enciphered the Washington signal it had to be deciphered in North Africa, and then the North African signal was enciphered there and deciphered in Washington. And was again

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

real-time operation. Rather simple procedure code had been developed for synchronization of the machines in giving the key settings because the key consisted in the selection of five wheels out of ten. These were reversible wheels so you set your basket with the five wheels. The stepping as I recall, well I found out it was a meterlike later, and the banding of course was an internal circuitry element of the basket containing the wheels and the banding is the connection are the connections between the end plate and the ~~Purnum~~ Vernam-type mixing device which mixed the cipher signal with the plain language signal both of them in the teletype mode. ~~After~~ About the time this circuit was established I got called away part-time from the cryptanalytic duties, ~~and~~ because of the scarcity of cryptanalysts who understood mechanical ~~things so I~~ and because I'd been involved with the ECM, I guess I was the candidate for this selection, the head of the War Department code room had set up a monitoring scheme in a little room separate from the code room, itself, in which he had spy machines which could be connected to the radio circuits so that you could print out on a printed slip whatever was being transmitted. ~~And~~ They normally used these spy machines to validate the operation of the cryptographic devices, the circuitry and other things. So when I went over to begin my twice weekly or so inspection of the code room at various times through the period of the assignment ~~and~~, I would go over sometimes in the daytime, sometimes on the night shift, and sometimes on the swing shift; just go in and putter around and look over the shoulders of the coderoom operators, and watch the radio transmitters work, and go in and take a look at the spy

TOP SECRET

machines, and just generally satisfy myself that the thing was operating smoothly and that I didn't see any cryptographic booboos appearing because ~~Yama~~ the Army Communications people looked about the proper operation of the circuitry. All I was interested in, were we making cryptographic violations because of misuse of the codes by the operators with the cipher machines; the ECMs being properly used; were the procedures the best; could we modify the procedures, for example, to make them more efficient? And these were the kind of general things we were looking for. There was no type job description for this. Just please take a look Frank, and if you see something wrong try to straighten it out. That was the general concept. Well I was I knew that the SIGCØM, thats what we called this new automatic teletype encipher device, the SIGCØM was going into use, so I selected that particular night at about the time it was going to be used to go take a look at it and see how it stood up. Well when I got over there I was a little disappointed. I found out that they had already started using the thing when the radio circuits first came up, they just couldn't wait. Stoner had put the pressure on them so I got there a little late. I didn't see the first operation. I watched this for a couple of days. I don't remember just how many days. But I do remember this - one night after I'd eaten dinner at home, I went over to the Pentagon which was oh, a couple of miles or so from Arlington Hall Station, went up to the code room and sat down in the room where the two spy machines had been installed and just watched what happened. I just sat there and watched, sort of feeling like I ought to put a good hard eye on those two spy machines.

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

to see just what was really taking place, not just a quick looksee, but a long, deep looksee. Well after about two hours of almost steady operation I saw something that really shook me up. I watched the spy tape come out of the printer head and these two spy machines were on the two-way circuits. One of the spy machines was on the Washington-North Africa circuit, and the other was on the North Africa-Washington circuit so you could see right there in front of you what was happening on both ends really. The signal on the Washington spy machine was taken off before it went on the air; the signal on the incoming circuit was at the equivalent point after it had been taken out of there but before it got into the code room. So I could see exactly what the enemy might be intercepting if the enemy intercept people were on these two circuits. Well, this thing that shook me up came about as follows: I saw the procedure signal go out from Washington - "Get set up". I had my little book there so I could see what he was saying. "Set up your wheels. I'm ready to transmit" I guess would be the equivalent. Then from the other end "OK" you see. "Set". They gave the indicator which disguised the initial alignment of the wheels, the five letters, one on each one of the wheels, was sort of the key setting for the wheels. And then I saw the signal come back from the other end, "OK". And "Go Ahead Please" GAPLS if you will and then I saw the transmission take place. Everything was beautiful up to this point of time. There wasn't a thing that I could be worried about. Then after about oh I'd say twentyfour to thirty inches of tape had gone through the tape had gone on to the circuit, I saw the spy machine covering the circuit from North Africa to Washington

send an "interrupt" ~~inner route~~ and the Washington transmission was broken, and there was word from the other end ~~which when I looked and~~ which I realized must have been "We've got a bust. Please retransmit", and I thought let's see how he handles this because this is a very critical thing. ~~and~~ I had my choice of going in and ~~say~~ saying "Be careful buddy", or I had my choice of leaving it up to him because he supposedly was trained the operator and just to see what would happen and if he did it right then everything would be good. Also it was just a little bit of a distance from the spy machines to where they actual transmitters were operated. ~~and~~ You had to travel 'round through a couple doors and down a corridor, so it would take a couple of minutes for me to get up and go down there -- and I just let it happen, because I wanted to see if these things were being done right. That was my job. Well, in due course the new transmission was made and I looked and compared the two tapes to see if it was identical. Whether the bust was on my end or the other end and obviously it was ~~on the other end~~ on my end because the two texts were different and the tape started spewing out. It took me a few seconds to realize this you see, and finally I thought well, gosh he's misset one of the wheels in the basket and that's the reason the fellow on the other end couldn't read him. ~~and~~ We got a retransmission of the identical text because it was tape punched you see, automatic tape, and here's a retransmission with a wheel offset, one of the wheels offset just one element, and that could be very dangerous depending on the internal wiring of the machine. ~~The~~ By the time I got around and told the operator we were having some possible trouble and please stop, the message had to go anyhow so it didn't really make too much difference whether it went in that version, and probably was a lot better ~~since~~ ~~HANDLE VIA COMINT CHANNELS ONLY~~ had already started

TOP SECRET

in this version to set up a third version and it didn't make any difference anyhow because I didn't get there in time to stop it. The damage was done. Well this bothered me. It took maybe ten minutes for the full impact of this thing to sink through to me and of course I had immediately recognized that this was a bad thing to happen. A favorable bust for the enemy cryptanalyst and I just hoped that I would have gotten one on some of their machines if I'd been in a similar circumstance. So I decided I'd better go back and see if I could determine just how bad the bust was. I didn't feel like stopping the rest of the transmission because I didn't have the hard evidence, if you will, to say that this bust is dangerous. But I got back to my office over in Arlington Hall Station with the spy tapes that I'd collected for the whole evening with these two bust tapes, if you will, that I had collected the last moment off the circuits, and sat down and started to analyze them. Now I knew the theory of the machine but I had not had time to study the internal wiring and how the ~~endplates~~ endplates were wired and how the rotors were wired and whether these were the best arrangements or not. I just didn't know. In fact I didn't know what the endplate wiring was and what the circuitry was, but I did know enough about the recovery of cipher wheels from that kind of an operation to feel like I might be able actually to recover the set of wheels. By early morning, around 2 or 3 o'clock I'd recovered the entire machine - the wiring of the wheels, the endplate wiring, and its operational connections to the mixing relay device. With this data I could have built a machine like it if I hadn't known about the machine. And what was my reaction? I went to the bathroom and wretched.

TOP SECRET

TOP SECRET

I was really sick because of the realization that if I could do this -- although I had the advantage of understanding the operation of the machine -- I knew and realized that there was enough information available from these busts so that a clever cryptanalyst, a clever German could duplicate what I did, maybe not as fast, but certainly it was inevitable that he could duplicate it. All they had to have was an intercept capability latched ~~down~~ on to these two circuits and the bust message together with enough text to carry on. I didn't have to try to read any other messages on that transmission because if I could go that far with the bust, I was certain I could put the others in. And then I had to decide what I was going to do at 2:30 in the morning with this information in front of me and I called Corderman who was the Commanding Officer, Arlington Hall Station and got him out of bed and got him to come over and see what I had done. Corderman was all shook up just like I was. He didn't wretch because he hadn't been working on the thing at high speed for 3 or 4 hours but he was just about as sick as I was and he took a decision that he would try to get in touch with General Stoner ~~and he~~ thought we ought to set up a meeting because there was no point in getting Stoner without the Army Communications Staff. Set up a meeting at the earliest possible time next morning and lay the whole thing in front of Stoner and say sort of -- ASA goofed and we've got to take this thing off the air. I was particularly chagrined because I was the little boy that sat down at Friedmans desk and put the idea forward and I was the foolish little boy that didn't follow through and take a look at the circuitry ~~of~~ which had been employed when the engineers had put the thing together. They did

~~HANDLE VIA COMINT CHANNELS ONLY~~
TOP SECRET

TOP SECRET

a beautiful engineering job, but they took that type of circuitry which was most efficient for their manufacture of the machine. It, from the cryptanalytic standpoint, was the worst that could have been selected. Now this is the relationship, the movement, the banding of the output endplate with the ~~Burnum~~ Vernam mixing device; ~~and~~ So I kind of felt like I committed a terrible crime. I don't know that I had committed a crime but ~~it~~ I just didn't do a good job I guess and it bothered me. Well I went home and tried to sleep. ~~and~~ I came back early next morning, and Leo Rosen had been working on the SIGTOT, the concept of using a one-time tape with you run a mixer just like we were using at the SIGCOM, so in effect we took the SIGCOM out and put in the one time tape and we were in business. We discussed this and I told Rosen about the awful thing that I had discovered early that morning. He didn't seem, he was shocked, but as he thought about it he said, Well, we got to do something. We got to put this thing through a test. We can't let it go out again. We must instead of immediately using it, we've got to reexamine the whole cryptographic connections inside the thing. ~~and~~ Of course this was absolutely what had to be done. We also recognized in our discussion that Stoner was going to put the pressure on us for an interim solution. ~~and~~ Rosen checked up on the status of the SIGTOT and came back before I left in the staff car to pick up Corderman in Headquarters Building to go up to the Pentagon. He (Rosen) came back with the report that he ~~felt~~ thought we were ready to go into production because the whole concept had been tested and the only thing needed was a tape factory to make a bunch of one-time tapes in quantity to get them over to North Africa and, of course, the Pentagon so that we could have two-way communication with the one-time tape replacing the two SIGCOM installations on each end. Then Corderman and

TOP SECRET

TOP SECRET

I got in the staff car together and left. I didn't have a chance to tell Corderman of my discussions with Rosen. In the first place we couldn't talk in the car because it was an enlisted man driver who wasn't cleared; and second we were under pressure to get there and make sure that I had my worksheets laid out for the meeting, so I didn't tell him about this replacement thing because we were so worried about producing the bad news we didn't take time out to discuss any possible good news that might be needed by Stoner and company. Well the meeting came off about 10 o'clock in the morning and General Stoner I recall sat down at the end of the table, a long conference table outside his office. Corderman and I sat down at the other end and I faced Stoner cause I was going to do the talking and the whole army communications staff, about a dozen officers mostly, well, the senior members of his staff were there because he sensed something dramatic was going to be presented. Well Corderman made the pitch that we had distressing news. The spy machines had revealed that there had been a bust and that by working overnight on it that one cryptanalyst, namely Rowlett here, was able to recover the entire machine, and feels like the German cryptanalysts could do it if they had the intercept ~~which~~ of the messages which went on that particular circuit last evening. And so I told Stoner what had happened. He and his staff had questions. When we got through Stoner had an awful black look on his face and I remember his exact words and they were to the effect "Rowlett I don't like what you've told me, but I know you and your reputation and I think you're honest man. I don't understand really

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

what you've explained but I think you know what you're doing and I'm going to take your word for it. Gentlemen we are going to take this SIGCOM out of operation right now and you and Matt Jones go and get started." Well I was a little bit afraid of Stoner because I was ~~what~~ about a captain and here he was a general officer, ~~and~~ but I knew what I had presented was solid. The next sort of important thing that happened was that he turned to Corderman and he said, "Now look Red, we been pumping money and manpower into that Army Security Agency of yours. You produced a device here that was a wonderful device, and you destroyed it. And you denied us the use of it. Mechanically and electrically from a communications standpoint it was ideal. Now I charged you with the responsibility for putting this as your first responsibility. You go back to Arlington Hall Station and you turn on your best people for this job and get me a replacement for the SIGCOM." Well I wished then at that point that I'd told Corderman, and I didn't know whether really I ought to go ahead and spill the story about what Rosen and I discussed that morning, but I also knew that if I didn't do it Stoner would be unhappy for a lot longer time, ~~and~~ I had enough confidence in what Rosen had promised so I just stepped out and laid it right on the table. That we could produce a one-time tape system that would operate as efficiently so far as communications were concerned as a SIGCOM. It did have the disadvantage though of the tape factory and I could speak with authority on that because of my earlier experience in the 134T1 tapes, and that the only hitch was to assemble enough gear to produce the tapes in quantity

and get them to North Africa. But I was sure that the whole thing could come to a head in the same time frame, but I had no way of determining whether it would be a month, a week or six months and the only way we'd know was to get started and when we got done we'd know how long it took us. I was giving myself enough latitude so I didn't get hooked with a date, and I certainly didn't want to hook Corderman on that date deadline. Stoner didn't hesitate. He said "Red, do it. Go ahead." Well I could tell about Corderman's distress because of the bind the whole agency was in, and I could tell about my own distress of having to step out in front of my boss and take the wand away from him. But it worked out beautifully, and in a matter of a few weeks we had SIGTOT working. The SIGCOM was examined. We put out best cryptanalysts who had not had a chance to look at this--Turner and Small--I got involved in it--Friedman was involved in a reexamination of the SIGCOM and we changed the wiring. We eliminated the fault that we'd found, and we changed the movement, and we put in an extra little gadget to further enhance its security, and with these modifications the SIGCOM came into being and was a useful machine for the rest of the war. I think this an important story because I don't know anywhere else in my experience where one individual was so deeply involved, say in the development of the concept, and then within a short period of time destroyed his own concept and denigrated it to the point of where it had to be reworked. Of course this left a question for us. Were the Germans able to intercept the SIGCOM messages that I had exploited--

because we knew that these would provide the answer they would be trying to seek? And did they in fact achieve any solution or success with the SIGCOM either at that time or later on because of what they had learned from this particular instance, or others which may have happened and that we didn't catch because there was nobody ~~else~~ knowledgeable looking at the spy machines? We did find the answer to that question. First question as I see it is, did they intercept the signal? The answer is when the TICOM team went into Germany they found no evidence the Germans had identified this circuit early enough in ~~the~~ its use as being an automatic encipherment circuit for them to become interested in time in it to pick up the bust. Evidently they did find the SIGTOT being used later on. What time I don't remember. So far as I know the Germans were never able to discriminate between the SIGTOT transmissions and the SIGCOM transmissions. ~~You~~ This becomes a little bit of a sophisticated technique in cryptanalysis. Our TICOM investigation ~~s~~ I believe clearly indicated that the Germans had not achieved this level of competence and this was of course fortunate for the allies, because had they achieved the level of competence that was demonstrated by the rather simple cryptanalytic operation that I had performed on the bust message, I think they would have been able to do a lot more with the allied automatic teleprinter transmissions which were enciphered by mechanical devices. I don't think they could have done anything at all with the SIGTOT which about the time that we put it into use became evident as the most secure of all systems that we were using in that timeframe

TOP SECRET

because the key could be randomly produced, and We knew full well the mathematics behind it and we knew how to use the random emissions from vacuum tubes and read this off so that the key was unpredictable, and We could mathematically prove that the key stream on the SIGTOT was pure, one-time, if you will, and totally unpredictable based on well understood physical laws. This is not true of rotor devices or any mechanical pinwheel device like the Hagelin which generates a kind of motor key and I don't think we had fully appreciated the significance of the mathematical provable randomness versus the device-generated, unpredictable key until we actually started using the SIGTOT. And what we did learn from the use of the SIGTOT was that we were most vulnerable when an individual used the same key twice or the same tape twice, but that wasn't news to us because we knew this was true of the Hagelin and all other devices which generated keys and applied them in a manner similar to that which the SIGTOT was used or even the Hagelin itself. Another interesting example of possible COMSEC hazards is found in what is commonly known as the Fellers Incident. I'll not repeat the full circumstances of the administrative arrangements that were made, but simply there was a ~~military observer~~ US military observer attached to the British forces in North Africa -- I believe it was known as Montgomery's headquarters. The purpose of this observer, and this was of course before Pearl Harbor and before the US was in the war, was to report back to G2, Washington whatever he thought was worthy of their knowing and to do this in whatever detail was necessary. Of course he had to use cryptographic

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

system to secure this information and the decision was made to use the current military intelligence code with its cipher tables for securing his reports when they were transmitted electrically to Washington. After his assignment and in due course in time, the British discovered that there was some leak which they finally identified as being centered around the daily war room briefings held in the British headquarters in North Africa. This is where the situation where the 24-hours was discussed, typical war room briefing and they were very much distressed about this and they began to search out to determine where this penetration might be and who was responsible for the Germans receiving this information and hopefully how the penetration was effected and how it was operating. After thoroughly scrutinizing the British officers who were privy to the information which was being compromised they came to the conclusion that it could not be one of the British officers, and the further conclusion that it must be the American military observer who either might have been an agent or that his reports either in North Africa or in Washington were falling into German hands. Obviously this was a very delicate matter which had to be dealt with in very diplomatic sort of way and the British approach to the Americans was carefully thought out, carefully phrased, and as I recall came through the Lord Halifax/White House levels initially. Of course when the implications of this approach, namely that could it be that the military observer's messages were falling into German hands which is the form that the approach took when it was made by Halifax's office to the appropriate people in the White House. It had to be relayed from the White House down to the Director of Intelligence, G2,

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

and normally would have come to the counterintelligence organization in G2 which in this case it did. G2's reaction was somewhat as follows: This could not happen in G2. It could not be Fellers. It must be the British and therefore we should respond that it is not an American leak. You had better go back and look at your own people because the only possible way we could have a leak is through our representative. We're convinced that he is secure and that the people on this end who read his reports are secure and they're not getting in the German hands. So we are not to blame. You are to blame. That was the answer. British didn't take this as without taking a further step. They made a reclama, ~~and~~ This time they inferred that our codes might have been violated by the Germans and through this channel, Halifax to the White House, the response came. This time because it involved cryptography-- the Chief Signals Officer became involved and I remember attending a meeting in his office in which G2 representatives and representatives of the Signals Intelligence Service, that's Col Bullock and Billy Friedman and myself sat and listened to the proposal of the British. ~~and~~ The response which was formulated was simply a reiteration of the previous response with the addition that not only are our people secure but our codes are secure. It must be your people and your codes Lord Halifax. I think Friedman and I were a little bit uneasy about this last answer because we had a little more savvy about the vulnerability of cryptographic systems, and ~~we~~ what the German and Italian cryptanalysts could do was ... we didn't know much about and I think we ascribe to them powers far beyond

TOP SECRET

TOP SECRET

what we later found out when the TICOM teams came back from their survey of German cryptanalytic, cryptologic efforts. After this cold response, very negative from the US the British took the bull by the horns and this is the interesting part of my story. Since they were reluctant to tell the true information that they had because they would have to reveal the source through the diplomatic channels, they took advantage of the fact that Kullback was on a TDY in London and because of the exchange on the Purple keys and JMA effort which was being conducted in B3, we'd set up a secure cryptographic channel of communication from B3 to the counter offices in GCHQ and Kully of course knew about this channel and knew that the information that came over this channel would be tightly held and never get into the command message center where it would be duplicated and spread throughout the communications file. So Kully did this. He sent me a message and it was a rather long message because he had quite a story to tell and the message substantially conveyed this information. The British had been reading the Enigma traffic from Berlin to North Africa. They had found in the decodes of the Enigma traffic what appear to be translations into German of reports filed by the military observer in North Africa, the U.S. military observer in North Africa. They have given me the text of three of these messages and urged me to call this the text of these messages and their concern about these reports to SIS, that's Signal Intelligence Service, attention. They feel that the American code has either been stolen or solved by the Germans and that these reports are the result of the interception and exploitation of the observers messages. They

TOP SECRET

urgently request that SIS undertake a review of the particulars of the use and security of the military intelligence code which the military observer is using, and to take whatever remedial measures are necessary to stop this most important and disastrous leak. These are my own words but this is what the message said and then there were three messages that came as annexes to this basic message. These were the British translations of the German messages which were sent from Berlin to North Africa and which in themselves were translations from English into German of the text of the reports that had been transmitted in the American code presumably. This message of course meant the following action had to be taken: first, we had to ascertain exactly what code was being used and what cipher tables for the encipher of this code had been used. This was easy. It could be only one code and the current cipher tables. The second was to determine if G2 had in fact could in fact identify the text of the messages as being the MA the military observers report. In order to do this we had to go through the Chief Signal Officer and the Director of Intelligence, so a meeting was arranged one Sunday morning because the message came in early Sunday morning promptly. A meeting was arranged between the Chief Signals Officer and those of us who had been involved and knew of the message Friedman, Bullock and myself from the SIS point of view and the appropriate people in G2. Well we presented Kully's message fortunately the G2 people who were involved had been cleared for the knowledge of our cryptanalytic capabilities and our liaison with the British cryptanalytic organization and so we could talk freely and explain how the message

See p 124

had come and validate its authenticity. G2 representatives however were not familiar with the reports and the first reaction was that this really couldn't happen. This was a defensive reaction. But it was clear that the way to test this out was to find from the code room in the war department message center if there were in fact messages bearing the numbers that were ascribed to these reports, and if they jibed the text of the messages bearing these numbers did in fact jibe with the text that the British had recovered and the German translation that they had intercepted. We found these messages in short order. The three messages identified by Kully in his transmission from GCHQ of the text and the British proposal. What did we do about it? Within 24 hours the military observer in the North Africa had received an ABA. A unique set of wheels. The ABA being the ECM. A unique set of wheels and two officers to train him and one officer to train him in its use and one officer to operate it for him. We heard no more about the incident.

91 → One of the often discussed mysteries of the early organization of the SIS is why Yardley was not brought back into the War Department to assist in the establishment or the Signal Intelligence Service. What I know about may help resolve some of the questions resulting from Yardley's not having been involved. In the first place, Yardley was a marked man so far as the Signal Intelligence Service was concerned because he was the key figure in the American Black Chamber and would immediately be identified as being associated with that kind of activity had he officially been employed by the War Department, and this would have destroyed the

TOP SECRET

cover that the G2 and Chief Signal Officer people had desired for the resurrection of the cryptanalytic capability within the War Department establishment. So it was almost impossible even to consider Yardley as having any contact with the rebirth of the cryptanalytic capability.

Tape 5,Side 2 This could be looked on as a mistake but I think events proved it was not a mistake because the way it actually developed the way the new Signal Intelligence Service actually developed proves that probably there was any advantage in starting afresh without being hampered by the desires and likes of the American Black Chamber. The American Black Chamber for example dealt mainly with manual systems solutions. The real breakaway, or breakthrough if you will, produced by the Signal Intelligence Service was as a result of Friedmans hope that we could mechanize encipherment and the result well the in due course the adoption of International Business Machines were assistants in the program co-production and later on the cryptanalytic effort and finally the development of the ~~Geewhizer~~ "Geechnizer" which was the first breakthrough into computery that I remember having seen in cryptanalytic operations anywhere, Army, Navy or UK. Now I think this adequately explains why Yardley was not employed in the development of the Signal Intelligence Service. Had Yardley not come into print with his book, The American Black Chamber, he might in due course have been brought in when it was considered safe; however because Yardley did publish the three articles in the Saturday Evening Post and I believe he got a thousand bucks for each one of these articles which was a pretty good sum in those days -- and had he not published The American Black Chamber, I believe he would

TOP SECRET

TOP SECRET

have been held in high esteem as a pioneer in signals intelligence. The fact that he did go into public print and the fact that a law was passed as a result of his publication of the information about the American Black Chamber put him on the black list across the board within the Army and Navy. In fact, when the liaison with the British was established shortly before well in the summer of before Pearl Harbor the British raised the question - What about Yardley, sort of? And the response of the US military establishment, I don't know what the Navy said, was ~~that~~ "that we want no part of him. We will not have him in our organization." Then the British asked the real question. Well, the Canadians have hired him to help organize a cryptanalytic bureau in Canada. What about that? The answer is, "If Yardley works for the Canadians we will have nothing to do with the Canadians as long as he works for them." I think this graphically represents the attitude of the Americans toward Yardley at that point in time. However, there are a couple of steps in between that ought to be talked about. One is when Yardley's book came out, Friedman was really excited and distressed because he felt knowing that Japanese was the number one priority of the ~~samll~~ small group he was charged with developing he felt that the Japanese would be put on the alert and that they would overhaul their cryptography and the result would be that we would have to rework and re-recover Japanese cryptography probably more difficult one than Yardley had been confronted with. His distress and emotion about this point I think was

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

well taken because we later found out the Japanese were extremely distressed about the Yardley revelations. They were so concerned about it that a translation of Yardley's Black Chamber into Japanese was made and it was put out in paperback form and sold for about 10¢ American on Japanese newstands. I know this because we ordered a set of them from Japan and it cost us very little for each one of the volumes. There is a copy of this Japanese version in the NSA library. This was Larry Clark's copy which he gave to me sort of as a personal gratuity and which I accepted only if I could at the time I left NSA let the library have it because it was then out of print and a very rare book and it seemed only right and proper that the NSA library would have a copy of the Japanese edition. The fact that they did publish this and some of the editorials that appeared in the Japanese newspapers which were reported on by the military attaches and the State Department representatives in Tokyo confirmed Friedman's fears and there was quite bit of excitement in both Japanese and diplomatic circles about these revelations particularly that part which dealt with the 5-5-3 ratio which Yardley tells about in his American Black Chamber. I think at this point in time Friedman became an activist operating against Yardley because one of the things he did was take a copy of the Black Chamber and he went through and he annotated it this copy. Charles Lindelson who had been on Yardley's staff and who before that time had been a great admirer of Yardley was also concerned about Yardley's revelation and he assisted Friedman in these annotations of the Yardley book. I think this would be an interesting historical item if that copy which Lindelson and Friedman worked on could

TOP SECRET

TOP SECRET

be recovered and made an example of history. I think it would throw a lot of light on the Yardley question and why wasn't he employed by the government in his cryptanalytic specialty. The other thing that Yardley did that further pushed him away from the possibility of employment with the government was that he took a contract with the Chinese in which he was to help the Chinese develop a cryptanalytic capability against the Japanese. By this time Yardley's family life had broken up and so he went to China where he worked for several months and actually was one of the last white men to come down the Burma road before the Japanese invasion. This was a rather perilous strip at that time because the road was not too well developed, so he barely got out. When he came back to Washington there was an official connection between Yardley and the government. General Akin who was the head of the War Plans and Training Division in consultation with G2 felt there might be some useful information that could be obtained from Yardley because of his being hired by the Chinese to work on Japanese military systems. At that time we had no military intercept of Japanese messages in quantities sufficient to allow us to make even an estimate of what kind of systems were to be used, and even in this timeframe it became evident that we began to sense sort of the inevitableness of war with Japan. Within the circle who were intimately concerned with the cryptanalytic activities and our concern was based more on being prepared to deal with Japanese military ciphers in case these hostilities broke out than it was with the fact of the hostilities. I want to make that point clear. We were more concerned of our incapability for dealing with Japanese ciphers in this event than we were with the realities of war because the evidence was pretty skimpy at that time, but the evidence was sufficient that it gave

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

us a certain feeling of urgency that this had to be done. I think these last two expressions put it in proper context. Well certain funds were made available to General Akin for making a contract with Yardley for some brochures in which he dealt with a variety of aspects of Japanese military codes and I believe copies of these can be found in the archives. I know there were at least four of them. The reason I know is because I was selected by Akin to be what was known in those days as a Contract Officer for these small contracts. Friedman was not selected because of his strong feeling about Yardley's book and I was pretty much neutral and a newcomer and a fresh face so it seemed to be more appropriate for me to deal with Yardley that anyone else because at that time I was in charge of the Japanese diplomatic section. Incidentally at that time Yardley's one-time secretary, Miss Rumsey had been hired by the Signal Corps and was working on the Japanese diplomatic section as one of the clerks doing clerical work cryptanalysis exploitation of the Japanese systems. I became very well acquainted with Yardley as a result of this Contract Officer relationship I had. I would inspect the brochures. I would discuss them with him. I would formulate questions which could be put to him because there were unclear parts in the brochures and that was part of the contract. It would be this clarification process. So I spent quite a bit of time with Yardley. I would meet with him in his apartment which was in just within the "F" Street area above the Munitions Building, and I'd usually go up early in the morning and take up whatever business matters I had with him. Yardley told me recounted

TOP SECRET

TOP SECRET

to me several times some of his personal experiences in working with the Chinese and I think probably the most significant of the yarns that he told ~~us~~ was about his relations with the Chinese intelligence service. He had probably 150 or 200 photographs which he had brought with him when he came out of China. These were photographs that had been provided to him by the Chinese intelligence service ~~and~~ The way the pictures were obtained was through the simple expedient of having extra copies made of any films developed by Chinese film processing laboratories that had been presented to them for processing by the Japanese occupational troops in the areas that the Japs had taken over. While this is not cryptographic in nature it was interesting that Yardley had a copy of that famous picture which was published in LIFE about the massacre of the Chinese and he had other examples of Japanese atrocities to both males and females which were unthinkable to somebody raised in America, extremely brutal treatment of humans with no regard for sex or human life. These pictures presumably had been made available by Yardley to G2 and I think showed that he was closely associated with Chinese intelligence. However the results which we got from these brochures were revealed to us certain aspects of Japanese cryptography. Of interest they were of very little technical use because Yardley was unable to make any progress at all in with his resources into the solution of the Japanese military systems, ~~and~~ probably this is the reason that he quit working for the Chinese and came back to America along with the fact that the situation was getting pretty rough out there. I don't think Yardley would have come back to America

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

if he'd started to be successful on Japanese, and I think this was the opinion that Akin and Friedman also accepted that about the considerations of Yardley's return. After we got the brochures and looked them over pretty carefully and examined them in the light of the intercept which is now starting to build up on Japanese military systems from our stations in the Philippines, we concluded that Yardley could offer us nothing and that the best course of action would be not to have him involved in the new effort that had been started in 1930. I don't think Friedman during his life ever ever forgave Yardley for going into public print.

Q: What was done in terms of developing traffic analysis in the early 1930s?

A: In early 1930s traffic analysis was not recognized. Traffic analysis was considered as a separate process, separate from interception and exploitation, cryptologic exploitation of intercept. Only after we had joined forces with the British and discovered that they had been able by setting the externals of certain German messages to arrive at certain intelligence conclusions which were valuable. On our side we'd had so much success with the systems that we'd been working on that we did not have to stop with the externals. We went in to the body of the message and therefore we considered the information from the externals trivial and something less than the less valid than the translation of the text. Our success had been great enough so that we never had to drop back and rely on the externals, so we while we were aware that some information could be produced by setting the externals, we didn't think we didn't find it necessary to undertake such a study in the formal sense that the

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

British finally developed when they had to deal with some systems which were invulnerable to their cryptanalytic effort and I think as I remember in discussing this with some of the more cryptanalytic minded people in GCHQ they also looked on traffic analysis as being measures employed in-between the successful exploitation of elements of traffic. If you couldn't read the message then you got what you could out of the externals, but when you start reading the message the externals were not as important as they were when you weren't reading the message.

Q: Where was the authority, the official authority, for tasking both in terms of targets and in specific systems? Where did that originate?

A: In what timeframe?

Q: In from the 30s up through December 7 again.

A: The best way to answer that question is to describe what I recall. As I mentioned in some of the other recordings the initial priorities were Japanese, that was the first, German was second, Italian was third, and everything else after these had been dealt with. So our first priority assignment, and the first task we undertook once Kully and Abe and Hurt and Rowlett had developed to the point of where they were ready to undertake active analysis of traffic, was to go back to the Yardley files which were in room 2742 Munitions Building, select from those files the Yardley worksheets and the intercepts of early Japanese messages and update the small force of the four people I mentioned together with Clark who had come in at that time in making an estimate of what had to be done on the Japanese first. Of course we'd done this research work on

TOP SECRET

TOP SECRET

ADFGDX which was a little bit of effort in terms of the second priority, but the first priority still remained Japanese. This is further reinforced by the intercept activities which in short were directed at the interception of Japanese diplomatic and military messages and of course wound up in that timeframe before the Japs went into China with only results in the Japanese diplomatic field because there just wasn't that much traffic on the air in the military for the US to intercept from the remote intercept stations it had in the Philippines. Now the basis for selection of Japanese first priority came from G2, and I suppose that we could say the translation of that priority into action was to start out with Japanese and see what could be done with it. Our first effort was to take that traffic out of the vault, bring it up to 3418, which was another vault in the Munitions Building, where to start with Kullback and Hurt -- Hurt because of his language capabilities and Kullback because he wasn't involved as Abe was in the preparation of military training material like Special Text 165 and 166 or like myself, I was involved, I was the co-production program, I was doing the cipher tables for the MI code. These had to be issued every three months. New codes had to be run in and out of the place and so Abe and I were kind of up to our necks in other things and Kully was the only free one, and the idea was that Kully and Hurt would make the first survey. Abe and I were involved in a little different way in that we had been taking Japanese training in Japanese, Japanese language, both spoken and written along with Kullback for several months, and we continued our study of Japanese, and It was Friedman's idea that after Kullback and Hurt had gotten this stuff organized and sort of found out what there was to work with and when they had defined the proper

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

set of traffic for us to work on starting with the Yardley Black Chamber material -- sort of going from the known into the unknown of current intercept -- that we would all become involved and this is exactly what happened. When Kully and Hurt organized and determined what was available and identified some unsolved messages that Yardley left behind we tried to go from the exploitable traffic, the time period of the exploitable traffic, into this unexploitable area and bridge the gap and hopefully use that as a further bridge to current intercept, ~~and~~ This is exactly the way ~~this~~ the thing developed. Now it was within a matter of six ~~to~~ eight months I think after Kully started looking at the Japanese material with Hurt that we made our first recoveries of Japanese two- and four-letter code charts. These were the old J series and fortunately in that particular era particular year, this was about '33 or '34, the full effects of Yardley's Black Chamber had not filtered down through the Japanese cryptographic service and they hadn't yet initiated this dreaded overhaul that Friedman had described as a horror story. So we were able then ~~to~~ sort of to carry the bull around while it was a calf, and we grew faster than the bull did because as we look further down to the point of where they began to introduce very unsophisticated transposition superciphers of some of these two- and four-letter charts, and the Red machine which I think was being used about 1932 in the Far East diplomatic net. Then that got distributed out of Tokyo to Washington, Berlin, London, Rome, Moscow, Ankara, ten all told, outstations. We were able to read everything except the Red machine, ~~and~~ Then of course Abe ~~they~~ had to go to Panama on ~~a~~ this special assignment ~~so~~ and Kully and I stayed behind and carryied on. ~~and~~ Since this batch of traffic which was later identified as being all Red machine

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

we went in to assist them, so at that point in time the total effort of the SIS was on Japanese diplomatic. Now when did we get started on German and Italian seems to be a proper question that ought to be answered. ~~and~~ When Abe came back from Panama that's Dr. Sinkov came back from Panama we had reached the point of where we were pretty well on top of all the Japanese diplomatic traffic, ~~and~~ I guess the reason that I was more mechanically inclined and more interested in cipher machines than the other two, I was given the Japanese problem, ~~and~~ we'd been getting some intercept in Italian and German and French, Mexican and other things as a result of this covering of the diplomatic circuits in response to the Japanese diplomatic interests that both G2 and we had because of our success, so the time had come to set up some kind of effort on the German and Italian which were #2 and #3 priorities, and then sort of everything else, so this kind of an action was taken. I don't think there was any direction to this from outside other than the statement of the priority and the order of priority because the implementation was left up to us in the Signal Intelligence Service and Friedman's decision with the approval of the war plans and training division was all that was necessary. G2 didn't know enough about what we were doing to make a judgement. I guess that is what it boils down to, and Friedman and his people did so they left it up to us, ~~and~~ the decision was taken that we will start then a German section and this for some reason ~~appealed~~ fell to Kullback although he was Spanish trained when he was hired, and the Italian section fell to Sinkov although he was French trained, and the rest of the world

TOP SECRET CHANNELS ONLY

TOP SECRET

TOP SECRET

the French, Mexican, South America fell to Frank ~~Beers~~ Bearce who'd come in a little later. I don't remember the rationale for this thing. I remember in my case I was real delighted that I was staying on with the old Red machine because there were certain things I wanted to do, and of course it was understood that we would all be working on everything; that nobody would be denied access to any of the other sections, ~~and~~ We'd gotten some money and we'd been able to increase the staff -- Bob Turner had been hired, Al Small had been hired, ~~Jean Kretchen~~ Gene Gretjan later ~~Jean~~ Gene [redacted] Feinstein, Mary Jo Dunning. We'd started turning out translations formally and we had to have a stenographic force. We had to have extra translator help, so we got a couple of those. We got military assignments like the language officers from Japan. We hired some Italian and German linguists and they began to come in ~~because~~ Now we're getting up in the timeframe where we considered war, that it was inevitable that some kind of a hostility would break out and we had better by God be ready. Now this goes back to a remark I made earlier in these recordings ~~that~~ about Yardley, that while we weren't sure the war was going to come on us we had to be prepared that it was, in the sense that it was ~~inventable and~~ inevitable -- so we went to work real hard in this direction. I guess to summarize and make a simple answer to a question that I turned into a very complicated one, that the way the priorities were given to the Signal Intelligence Service, without any binding instructions as to how to use the resources in response to these priorities, was the first step in the organization of the effort, ~~and~~ the second step in the organization of the effort was

[redacted] CHANNELS ONLY

TOP SECRET

the utilization of what resources were available, both intercept and manpower, in such a way that the most efficient utilization and production and exploitation could be achieved.

Q: Did this situation change once the war actually began and we became involved in it?

A: Yes and for a new set of reasons. The Japanese diplomatic effort had been pretty well cleared up when we finished the solution of the Purple and it was more of a sustaining effort at that time because if you're producing good intelligence people sort of leave you alone. Now when Pearl Harbor came into being, G2 was aware that there was a going effort in the SIS in terms of Kully's work on the German; there was a going effort in terms of Abe and his section's work on the Italian; and Bearce's outfit on the rest of the world. They also knew that we were making a rather broad study of cipher machines. This was again my responsibility because I had the machine experts in the terms of Förner, Small, Snyder, Rosen was very closely associated with the Japanese outfit because here was the live, living traffic that you could practice on you see and the prize was great intelligence, ~~and~~ so they were aware that we were pretty well out in front technically and ready to deal with whatever we could get our hands on in terms of intercept. Now when war, when Pearl Harbor happened, then of course everybody got excited and wanted the answer day before yesterday. Now this generated problems from the concept on which your question is based. We did have to make a reexamination of our effort and what this amounted to in that timeframe is that we could ill afford to stop what was going because in all the sections, in the German section, and in Abe's section in particular, they could not

afford to lose the momentum which had been built up when they were able to spend more time with research. Also, there was a tremendous increase in the intercept for two reasons. One, we had built up a greater intercept capability within the U.S. Granted it was still in a poor state of training. But we also had a mass of material we were getting from the UK, you see, because they had a well organized, active and well trained, as well as productive intercept activity, so with the initiation of the liaison with GCHQ we just got a massive amount of traffic. Also in Kully's case there was the work that the British had done in terms of the analysis of the I'll call it the Floradora system, that was the double additive system that was less than the one we later identified as the one-time system and called GEE and so there was the technical information that Kully got. There was a similar batch of information from what Abe got ~~and~~ in his work on Italian, and then the rest of the world, the French and so on, of course by this time the French, the only thing left in the French was the Vichy government. But there was another development -- that is the interest in the Turkish, and the Near East and the Middle East and what was going on down there, and so we were ~~beginning~~ being propelled into a situation which would embrace all the important nations of the world whether they're big or little with particular emphasis on the Middle East and South America. Now the positive action which had to be taken was to get enough people on board and enough skills particularly language skills to begin undertaking some kind of a positive and formal effort in, for example, nations in the Middle

East and the rest of the world, ~~and~~ this is where a great contribution was made as a result of our liaison with GCHQ. As a part of the deal, Carter ~~Clake~~ Clark had argued that we ought to get access to every damn thing that the British had been successful in, ~~and~~ he wouldn't play ball unless we got it and he made it stick, ~~and~~ the British came over and gave us everything except the Enigma and some of the clandestine effort on ~~the~~ German clandestine traffic, ~~and~~ I think in some of the literature on this question some misunderstanding has resulted about the British how free the British were in their exchange. I can tell you that I saw it from the inside and that the British clearly gave us everything except the Enigma and the clandestine, and they were reluctant to do this because of the very tight security which they had surrounded this effort and they felt it was untimely unless we could use it, unless we were actively in need of the intelligence from the German Enigma, ~~and~~ Of course we had no CIA or clandestine intelligence service capability at that time -- Just what the Bureau was doing and that was an exchange of the translations on that. There was a fellow by the name of Simperman, FBI representative in London, who as a result of this exchange got the results of the British clandestine effort. So ~~we were pretty well~~ we were pretty well satisfied even on these two areas they withheld, and I think our relations with them as time went on resulted in the British Navy building a typical Bombe over at the NSS for exploiting German naval traffic because we argued that we ought to have this capability in case England did in fact fall, ~~and~~ We went to the relay mechanism known as Madam X in the basement of B Building. Now to summarize what

FBI

TOP SECRET

we did was sort of follow our nose taking advantage of each break, each opportunity to expand the effort for any one country using the existing organizational structure with a full freedom of flow of our technical people from one area to another including, as I've told you in my case flowing back and forth between the COMSEC. So we really just grew like Topsy I guess is the proper adjective.

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

Pages 144 & 145 not used

TOP SECRET

Tape 6, Side 2 | The question is what was the basis for the nomenclature of U.S. devices as exemplified by the term SIGCOM, SIGABA, M134T1, T2, T3, and T4, etc. A little chronological review. Prior to 1930 the concept of covernames had not been developed and usually a short title, an abbreviated title, was used to describe a development. An example of the pre-1930 attitude is found in Cipher Device Type M94 which was abbreviated to CDM94 which taken just the five elements or so ~~as~~ is a nonsense group. But if you expand it its just the initials for "Cipher Device" Type M94. Now when we get down to the ~~early~~ earliest model of the M134 which went in effect, we find this title was ascribed to the machine about 1930 ~~and~~ ~~and~~ Friedman and the signal ~~officers~~ officers were getting a little bit nervous about the use of the term CD or "Cipher Device" so they just simply tagged on the M, as (in) M134, meaning Model of machine 134 and you identified the cipher machines out of the rest of the development contracts because ~~as~~ in the other case they continued the abbreviation process. So it was no abbreviation, It was a cryptographic development. In about the period of 1938 - 39 there were quite a number of new devices being developed and it became necessary to do two things. One, is to have a meaningful designation for a cryptographic device or system, and a secure designation. So a list of pseudo code words was generated using the term SIG as the first three letters followed by another three letter group as in the case of SIGABA, S-I-G-A-B-A was cipher machine or cryptographic device or Signal Intelligence, Source device, A-B-A, and ~~they~~ we get on down, and the next one that comes to mind is SIGCOM you see which was subsequent to it. So in this list which had been generated and probably can be found somewhere in the

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

COMSEC archives you can identify the short titles of SIGABA, SIGCOM and SIGTOT which is another example that ~~is~~ sort of as time goes on the alphabetical progression is effectively chronological and in the order that the concepts were advanced. Now the Navy did not adopt this system. They used their own nomenclature. For example, the ECM which is the Navy nomenclature for what we in the Army called the SIGABA is Navy terminology. So the ECM and the SIGABA are identical devices. To go back to the earlier system of nomenclature I mentioned the 134 -- M134. I remember being confronted with the problem ~~in~~ one day when Friedman was absent. We were required to I was asked the War Plans and Training Division was required to produce a secure title for a cipher machine that didn't reveal ~~that~~ it was a cipher machine because they didn't want the unauthorized people to know really how many cipher machines we had had to develop. So I was asked what we could use in lieu of the term cipher device or cipher machine, as we found in the case of the M94, which wouldn't mislead or disguise the fact that it was a cipher machine. At the same time we wanted something meaningful. I think I proposed the word converter because it converted plain language into cipher text and this delighted everybody so we started calling the 134, "Converter M134" and of course M is Model. So if you find the word converter its obviously a cipher machine ~~and~~ if in fact its date is before the inauguration of the SIGABA, SIGCOM, SIGTOT nomenclature series. The question is what do I know about direction finding in the 1930s. There was some direction finding effort undertaken by the Signal Corps laboratories at Monmouth the development of radio goniometric apparatus. I remember also on the occasion of a trip to Monmouth, which was part of

Q.
A:

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

our indoctrination and training during the early 30s, that I'd gone out to examine a field installation that had been set up by the Signal Corps Laboratories under the auspices of the, then being born, Second Signal Service Company who was operating this DF installation ~~and it~~ was a portable type of device. It had a loop, a small loop which was mounted on a 1x2x3 metal case which contained the electronics. ~~and it had a~~ The loop could be rotated 360° and had gradations degree gradations marked around it just like on a transit head, ~~and~~ So by turning the receiver ~~of the~~ contained in the lower box and by rotating the loop you could approximate the direction from which the signal was coming. I remember particularly ~~the technical aspect~~ one technical point that came up in connection with it and this was a ~~great deal~~ great suprise to the operators and the officer in charge of the test. They found if they moved out on top of a hill that they got one kind of a reading, then moving directly away from this reading down into a meadow along the side road they got another reading. ~~and~~ Later on when I learned a little bit more about direction finding, I remembered that ~~the~~ there was a power line along the second location. ~~and~~ It didn't occur to any of us at that time, either myself as an observer or the people who were operating the set, that the direction could have been distorted by the presence of the power line. I mention this sort of as an indication of the understanding of the state-of-the-art. We had no people in the Second Signal Service who had any understanding or experience of the principles of radio

TOP SECRET

goniometry, and we as cryptanalysts had very little interest in the mechanics of it, but we had great interest in a direction finding in order to determine the location of radio stations and other things for intercept purposes. But we considered this beyond our responsibilities. Now later on several contracts were let by the Signal Corps, and by the beginning of WWII there was quite an effort and a great deal of sophistication in this area. Question is where there teletypes in operation on December 7, how many and where were they located? On December 7 there were two circuits in being. They had not been activated previously. I'm now talking about the Army Security Service. Not the Navy. The Navy had other circuits and I will leave the answer to what the Navy had to somebody who knows more about it, but I know what the Army had and we had a circuit to Presidio, ~~Poidio~~, the intercept station out in California, and one to Station One at Fort Monmouth, New Jersey. We had had these installed these teletype installations installed and I guess if you want to know how many machines there are there were four machines because there was a machine on either end of each of the two circuits. So we had one installation in San Francisco, one machine, one in Monmouth, an installation with one machine and an installation in Washington with two machines, one for each of the two separate circuits. These two circuits were to only two of the intercept stations. The ones which we figured were most important in covering the Japanese diplomatic message circuits. The one in San Francisco was very close of course to the West Coast Transpacific terminal of RCA and the one up in Monmouth was very close

to the Transatlantic terminal out I believe its out on Long Island - east of New York City, and so these two stations would enable us to intercept the transpacific commercial circuits and the transatlantic commercial circuits, and that's why these two were chosen as the initial installation? We had contemplated and if Pearl Harbor hadn't happened we'd probably in a few months would have had intercept teletype service with Fort Hunt because it was close enough that we could tolerate a courier trip which was performed by Lt. Shucraft later he was Col Schukraft Shucraft, and a very knowledgeable man in the intercept exploitation areas of SIGINT. Pearl Harbor however changed the picture and we took the simple plans, our contemplated arrangement and lost sight of in the expansion of the intercept service because its character suddenly changed from being interested primarily in diplomatic to what to do about Japanese military and what to do about, in the case of the Navy, the Japanese navy, and so there was quite a readjustment and replanning and a terrificly rapid augmentation of intercept facilities. The two teletype circuits between Washington and Psidio Presidio and Monmouth were activated after the announcement had been intercepted and translated and delivered to G2 that the 14-part message was going to be transmitted, and the reason we activated or tried to activate, and I will talk more about that in a short while, ~~at least~~ this reason ~~when~~ we tried to activate these two circuits was to insure rapid delivery of whatever intercept particularly from Psidio Presidio could be obtained because we thought the message would come in through that link and this was the fastest way of getting it that we knew of. Shucraft and I were the ones who activated these two links because we did not know how otherwise to expedite the processing of this message once it had been intercepted except to use the teletype link from San Francisco. If we didn't get it

from San Francisco ~~over~~ by the teletype link it would have been would have required the mailing of the intercepts from ~~Psidio~~ the Presidio to Washington, ~~and~~ So we were very anxious to get them in a hurry and this gave us a very strong motivation to get that circuit into operation. We did raise San Francisco and we got a response, but unfortunately, in the case of the message that we were desirous of receiving rapidly, the intercept station had already sent its batch of traffic down to the mail room in ~~Psidio~~ the Presidio and it took something like three quarters of an hour for them to retrieve the traffic and poke it up and put it on the line coming back to Washington. In the case of Monmouth, I recall this, ~~as~~ it's a little bit amusing today but it was a very disheartening situation when I learned about it. ~~Shuc~~Schukraft was extremely distressed, but the officer in charge of the intercept station when the ~~intercept~~ installation was made, as a precautionary measure, warned all the enlisted personnel not to touch this machine, to leave it alone unless he was there and was insuring that it worked. Now when we tried to call up from Washington to activate the circuit to Monmouth, this officer was not present. ~~and~~ The enlisted man, who was in charge of the intercept activity heard the bell which normally rang in the callup and ask you for a response, heard the bell ringing and of course the machine was plugged in and the power was on, it was operating for a callup. So after being annoyed by this bell ringing for some time over in the corner ~~where he where~~ the office in which he was located, he gets up and pulls the plug and the machine quits ringing its bell and nothing happens. I don't suppose ~~Shuc~~Schukraft and I thought about calling up on the telephone to see what was wrong but we sort of didn't worry

too much about Monmouth after we had raised San Francisco because Monmouth didn't seem to be ~~too~~ as important in satisfying our desire to pick up this 14-parter as evidently San Francisco would be because of its location right in the line of the transpacific radio circuit. Of course this was a little bit of departure. The activation or the attempt to activate these circuits was a little bit of departure from the other arrangements we had for rapid delivery of traffic. The fastest way we had of getting an intercept to work on was to pick it up, intercept it at Fort Hunt which was just a couple of miles down the river from Washington and courier, send it up by courier from the intercept station to Washington. ~~Shuerafft~~ Schukraft when the pressure was on would make three or four trips a day down picking up the messages bringing the important ones, and in some cases he'd kind of wait around until the circuit closed down and bring the whole load for the day so we were working on messages that had been only minutes, well just the time it took to get it off out of the intercept operators typewriter and for him to bring it up to the Munitions Building and log it in. We religiously logged every message that came in and I 'm glad we did because this was a wonderful thing in terms of the Pearl Harbor inquiry that came later. We could locate whether or not we had found the message, we had the message, what happened to it and where it was in the processing, what the well, we could go back in the translation to the intercept copy and this was extremely important from the Army standpoint in answering the questions about the ~~Winds Execute~~ "Winds Execute" message. Now that was our best source of intercept -- most promptly received source of intercept. And then there was another very important, vital

TOP SECRET

source of intercept and that was found in the pickup arrangement we'd worked out with the local RCA office in Washington and the other cable outlets that we could trust. Early each morning an officer in civilian clothes this was primarily 1stLt. Earle F. Cook who later became Chief Signal Officer. It was his duty, when he was assigned to SIS, to go to the cable company, pick up the messages that he had worked out an arrangement to have held for him and I believe that they had an extra copy, I'm not sure, they had an accounting copy and before it went to the accounting office why Cook was given access to it. And he had a little cubbyhole sort of under a stairway somewhere in the building and in there he had a little installation consisting of a 35mm Kodak with a closeup lens and a couple of lights. I think they had a package Kodak sold in those days and we bought one ~~and bought one~~ and put it up there in this little room and he would photograph these messages just like Cicero did in Five Fingers and we could see his fingers on many of the messages, and then turn back the accounting copy to his friend in the cable office and bring the undeveloped rolls of film in his pocket and briefcase down to the Munitions Building where we'd run them through a little dark room laboratory set up that we had right next to the cryptanalytic office and run off a prints in a fairly short length of time. These were very good copies. They were garble-free and sometimes they were useful, not so much in the case of the Japanese in the example that I'm going to cite, but in the case of some of the work we were doing on Hagelin machines and other things because sometimes a notation would be made on the copy which was filed by the code clerk which was useful ~~which was useful~~ in our

TOP SECRET UMBRA ONLY
TOP SECRET

TOP SECRET

cryptanalytic work. He'd make a little pencil notation and sometimes he would rub it out, sometimes he'd leave it on and this would tell us a little bit about the setting of the machines and the wheels and the type of device. For example, there was no doubt that the Norwegians were using the Hagelin machine and the Swedes were also using the Hagelin machine because they had prepared the message blanks by pasting up the little gum slip of paper that comes out of the cryptographic Hagelin device itself. So there was a little bit of aside benefit from this photographic intercept activity. We didn't have as I recall right now, I don't think we had any other but the Washington. Question is what was the legal status of this so-called photographic intercept through obtaining copies from the cable companies? The answer is, and you can also find this in the Pearl Harbor report, that this was strictly illegal. It was against the law and it goes back to the law that was passed whenever Yardley issued his Black Chamber, and this is where the boot came back to bite us. However if you will look it up in the Pearl Harbor report, look up the reference in the Pearl Harbor report to this question you will find that the congressional reports commends the U.S. military installations for its foresight and initiative in undertaking this clandestine procurement although it was a very illegal, totally illegal operation, commends the military for undertaking this effort. When the group was organized in 1930 very little thought evidently had been given to background, well sort of to be brutally frank no thought had been given to such things as background investigations and security clearances or the other things which seem to

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

have developed as a result of our becoming more sophisticated and assuring ourselves of the security of individuals. What happened is I think about the limit that could be expected in those days. I believe Friedman and Crawford in their selection of those of us who joined the Signal Intelligence Service were quite satisfied. For example in my case to see that I was a mountain boy from the heart of Southwest Virginia and it was most unlikely that I would be have any loyalties except to the United States. Same thing I think applied to Hurt and to Sinkov and Kullback, and Larry Clark was a son of a metropolitan policemen. So you see our family connections, where we were born, and we were all obviously born in this country, although Friedman wasn't, he was born in Russia, seemed to satisfy the what then was thought to be a security requirement. Indoctrination? The indoctrination that I got the first day that I arrived on board was after I had been processed and taken the oath of office, which was a very simple thing in those days, later on I was fingerprinted but wasn't given any priority at all. When I was introduced to Major Crawford, later General Crawford, he was then the head of the War Plans and Training Division, so we talked, he was very pleasant, welcomed me and had some words to say and asked some questions. And then he sort of leaned back and put his hands behind his head in his chair which was a swivel chair with a spring in it and looked at me very sharply through his rimless glasses and said something to the effect that, "Young man you are not to talk about your duties in this office. If anybody asks you what you are doing tell them you are working for the Chief Signal Officer. And if they ask the nature of your work tell them

TOP SECRET

TOP SECRET

its statistical and mathematical. And if they ask you any more embarrassing questions lie to them as best you can." And these instructions were reinforced by Friedman a couple of times and then finally they wore out because we began to laugh at them when they gave us these indoctrinations, and actually I did find it necessary on occasion to actually to fabricate stories explaining why was a mathematician in the office of the Chief Signal Officer and my answer was we were doing statistical work you see on message counts. We had to do certain statistical analyses of these in terms of routing of messages and this was a little bit too much for the average friend I had in those days so they dropped the question. We never mentioned codes and ciphers and really my wife had very little idea of what my whole career was until I retired and she was she read some of the remarks that had been made both in connection with the publicity which I got before I retired. So she was a little surprised at what she learned about me. It is interesting to note that this kind of close knit group we had a very tight personal relationships -- Friedman and those of us who were working for him, and coupled with sort of a clandestine nature of code breaking, made us more security conscious than all the indoctrination could have been given us by Friedman, Crawford or anybody in those times because we were developing our own understanding of the need for secrecy and particularly when we began having some success you see, breaking the Japanese diplomatic codes we didn't want to have to go through that ordeal again because Friedman had made such a horror story out of the Yardley book that we could imagine we might become Yardleys. One of the most interesting post-war efforts that I remember was what we call the TICOM effort. The five-

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

letter group TICOM stands for Target Intelligence Committee, and I forget what the O, well, thats what T-I, Intelligence, C-O-M, ~~COM~~ Committee. And this was generated by a British concept. They seemed to be a little bit more clever about these things in those days than we the Americans were because they thought it would be a wonderful thing to have a team of knowledgeable people, experts if you will, poised ready to go in and occupy and examine and latch on to the files of installations that had been involved in cryptanalytic and cryptographic work in Germany. These had been carefully pinpointed -- accurately pinpointed through their intercept work and other intelligence reporting so they knew exactly where they were, ~~and~~ they had a plan and had developed sort of a project, I believe we called it a project, to uncover, to occupy, to go in and take control of these installations at the earliest possible moment after they had been enveloped by the invading and attacking forces, the American Allied Forces. Well, we collaborated with the British in this and there was full cooperation and we had quite a party for both the Army and Navy at Bletchley Park and we designated some of our better people in both services to join with the selected group of Britishers. We placed emphasis on knowledge of German because we wanted any interrogation to be done as close to the language as possible. ~~and~~ We had interpreters as well as experts to reinforce this language problem, ~~and~~ as we began to see the German resistance disintegrating then we were ready and we did assemble these teams together, ~~and~~ We had them just behind the forces so each time one of these installations was overrun there was a group of cryptologic experts right in there interrogating the people who were who had been doing the work for the German intelligence services. Among those I remember, Oliver Kirby was one of the Americans who went on this. I believe Roy Johnson I understand Roy is dead now,

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

but Roy went along on that and some others. I was greatly disappointed because I wanted to go and Corderman wouldn't let me. He said I need somebody here to help clean up this mess. The people are all going to be leaving and you're stuck buddy. So I didn't get to go, I wish I had. I could've have gotten by on my college German probably. Now to get back to business, the teams did go in and I mentioned in the SIGCOM ~~reporting~~ recording that we made how we had learned that the Germans were not too successful in discriminating between the SIGTOT and SIGCOM traffic. This we learned that was useful. We also were very much interested in what results would have been what results have been achieved by the Germans on the ECM or the SIGABA. And we got the answer to that. I think its an amusing answer and I will put it in my own way as more of a joke. But Art Levinson who I believe was on this team, and I believe it was Art who reported to me when they talked to the fellow who was in charge of what they called the American Big Machine, see they'd identified the Big Machine as the one jointly used by the Army and Navy. They couldn't tell we were using different rotors or other things because their cryptanalytic understanding was just not at that level and that was an interesting item in itself. But Art's report as I recall was that they found this guy inebriated and his co-workers reported that he had turned into a dipsomaniac because of his lack of success on this "American Big Machine". They did have some success with the Hagelin which was used with the US Air Force and I'm awful sorry we didn't have a better device. Of course maybe we were lucky, not we even had that because enciphering our

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

communications in the timeframe thats permitted by rapidly flying airplane with something that the state-of-the-art just couldn't accommodate in WWII. So we fell flat of our faces in providing secure communications there. Now this weakness of air-to-ground communications was more critical in the Pacific because the Japs took advantage of the voice-to-ground communications and actually destroyed planes because of the indiscretions made by the pilots. I believe thats documented somewhere in the history. I recall it as one of the bad aspects of our work. Now of course the experience with Germany and the grand results which we obtained the insight into not only the Germans but what they'd obtained from the Italians, the collaboration with the Fins, the Japanese which we already knew a little about because of our reading the Japanese military attache system was terrific information. It gave us a little better feel for the relative competence of the U.S. and the UK organizations which had about lifted each other to ~~about~~ the same level. I mean where we were deficient in additive recovery and things like that the British were very skilled. They were not as clever in the machine cipher solution as we were, and I think our cryptography was -- because of the ECM and the SIGTOT well, mainly because the ECM, because the ECM was a much better and more reliable device both cryptographically and from the engineering and operating standpoints provided by the IT&T engineers, much in advance of the Type X. The British did have a machine which they inadvertently showed to me and to Leo Rosen and as Sir Edward Travis once put it "He couldn't have picked two worse guys to have it shown to." Quite by mistake they showed us a new device. I forget the

TOP SECRET

name of it. It was all in chrome and black and was demonstrated both to Rosen and me. Rosen I don't know what date he saw it, but I saw the first time I went to Britain, ~~and~~ I guess the reason I saw it is because I was a cipher machine expert and they felt they had to show me all the machines. But nobody had told them, "Don't show them the British machine." It was a pretty good machine. Actually they installed it between the in America first between New York office and Washington and the British office in Ottawa. And then they used within well between Britain and the continent after "D-Day" because it was before D-Day that I saw the thing. Well to get back to TICOM a little more about it. It might be interesting that we had truck load after truck load of German cryptographic equipment. We had Geheimschreiber and Type X's, naval, air. We had commercial Enigmas. I'm sorry. I mean Enigma not Type X. Type X is the British machine and we had the naval Enigmas, the military Enigmas, the air Enigmas, commercial Enigmas. We had some forward looking developments in the German cryptography that hadn't come into being. We had some of the technical reports right up to the solution of ~~books~~ codes and ciphers of other countries, photographic copies of second-story jobs that they had performed on safes and embassy coderooms, and a whole variety of stuff like that. This was gone over, carefully evaluated and assessed, and a series of reports produced which you might find under the term TICOM Reports. To add my own personal evaluation of this thing, it was a wonderful thing to have this insight into what the Germans and Italians well, particularly what the Germans had been doing. And I think

TOP SECRET

TOP SECRET

its a proper commentary on Germans the German approach in that they had seven separate and identifiable COMINT organizations each in competition with all the others, and I would hazard a guess that they could have done a lot better if they had a unified central cryptanalytic organization which was politically impossible in those days the way Germany and the German government was organized and the SSS and the Hesses and the Canarises all sort of looking with great suspicion on the others. Now a few words about the effort in Japan, after we had seen how wonderful this work was in terms of the German TICOM efforts. We thought we'd better do the same thing when Japan surrendered so we sent in some teams. These were mainly taken from the force down in Australia. Hugh Erskine I believe was the head of the American team. Larry Clarke was on it. I don't know whether Abe was involved in this or not. I think he came on back to the States pretty soon, but Hugh was very good for this because ~~High~~ Hugh was excellent in Japanese. He could do the interrogation. ~~and~~ We'd provide them with a list of questions including ~~what~~ what about the ~~Winds~~ Winds (?) message, and I think Hugh's report in TICOM will speak for itself. We also, I don't believe it was through TICOM but we picked up pretty late in the war when we overran the Philippines, we picked up a new Japanese cipher machine that was entirely different from anything else we'd seen. The Purple. It was more like a sort of a cross between the Enigma and the Japanese version of a rotor machine. Strictly Japanese. No resemblance at all to the US ECM but I believe it had a something like ten wheels, eight or ten wheels and a lot of controls.

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

It's described also in the we used to have it in the musuem if there is a museum around it can be cited. I think it's interesting to sort review what the attitude of the upper echelons of the War Department were towards this newly born Signal Intelligence Service. Very few people knew about it outside of the people who were involved. Those were the Chief Signal officer -- of course he was directly involved administratively but technically and operationally was not involved; The Director of Intelligence, G-2, the communications desk G-2 were involved in the planning and there wasn't much anybody could do except support the effort until it had proved that it was going to be capable of producing results. Now G-2's attitude in the early days when we were being trained was "Let's leave them alone until they learn they can and then we'll put the pressure on them. We'll start working on the Japanese and then when they find out what they can do on the Japanese then we'll go to German and Italian." So G-2 was very generous to us in those early years and I think it was to our benefit and to the benefit of the effort that they took this attitude. This was sort of the status until we began reading some of the Red Machine messages which let show through a the glimmer of the German, Japanese and Italian tripartite pact. That was the most exciting thing that I can remember, The thing that really got G-2 up on its ears, ~~and~~ Johnny Hurt turned out a translation one afternoon of a partially recovered code message in which this was mentioned and we sent down ~~an attempted~~ a tentative translation. Col. ~~Blackman~~ Bratton was up the next morning waiting for us to open when we opened the office to verify the translation. He wanted to see the Japanese text. When he saw the kind of meager

TOP SECRET

recoveries that Hurt had used to make this tentative translation he went away sort of shaking his head and said, "I wish we had more of that text recovered boys. Please get to work on it." Now you see when they began to get these nice tidbits and morsels they suddenly developed an interest in speeding up the operation because they wanted to get more and more information. Well this was this pressure was applied in a very friendly and benign way, thank the Lord. They didn't go up and crack the whip of the Chief Signal Officer and issue orders to read those code messages yesterday boys. They just had more sense in those days than to do that kind of thing because I think they had a feeling they were lucky to have anything any prospect of dealing with future intelligence production. So they left us pretty much alone and just encouraged us. That was attitude. And then of course when the Red Machine was broken why then they began to be more specific in their requests. They say "Translate these mesaages from Tokyo to Washington before you translate the ones from Tokyo to Ankara, for example." And they began to sort of lead us, not by orders, but say sort of "We would like to have it this way instead of the way you're doing it." And that was a healthy thing. And the next step because they could get Japanese language officers like Carlisle and Joe and others, Spenson and Munson, Freddy Munson, General Freddy Munson was one of them. They'd get them assigned to and they'd detail them up to Signal Intelligence Service as translators, and then the military language officer who was assigned to the SIS would perform the selection

TOP SECRET

duty that is what messages were to be translated. We just funneled all the messages across his desk and he'd sort of make a little note on them like this message is about ~~Caruso's~~ Kurusu's conversations with ~~Peru~~ Grew or with Hull or foreign ministers discussions with Grew on this subject sort of indicate whether it should be done immediately or not translated, or held in abeyance and translated when time was available. Now this was a useful thing. Quite a natural development. We could live with it without a bit of trouble and G-2 could live with it. But at that time there was not the very urgent pressure for the general flow of intelligence, just ~~new~~ little items about the Tripartite pact and things, goodies, morsels of interest. Now we're getting up to about the time the Purple went into use, and then we felt a little bit stronger pressure to get on with the reading of ~~the~~ this Purple because the traffic ~~in~~ between Tokyo and the holders of the Purple machine, the real good intelligence, the kind of discussions I mentioned about the tripartite arrangements, they were lost because they were in this unsolved system. And so I wish you could read that new machine is what they'd say to Friedman and the Chief Signal Officer, or. When we read that new machine we will have a better insight into some of these arrangements. This was a friendly pressure. We were sort of family. There was nothing in opposition between the G-2 in the '30s and the Signal Intelligence Section of the '30s. Now I'm probably spending too much time on this, but I think it was a healthy thing and contributed a great deal to expediting our development because they could have hampered us by placing requirements. I'm sure that if they had pushed us on the Japanese that Kully would not have made the progress

~~TOP SECRET~~ ~~TOP SECRET~~

TOP SECRET

in his German section nor would have Abe in the Italian or Bearce in his other responsibilities but they let us do it the best way we could and sort of in our own way under their general request that this is the kind of thing we want. Now when war became imminent we began to feel this a little bit stronger because G2 got an augmentation in intelligence officer assignments ~~and~~ unfortunately the amount of training in intellligence to make a proper intelligence officer. There was nothing. There was no training of intelligence officers. If you were a Japanese language student then you got assigned to the Japanese desk. If you were a German student you got assigned to the German desk ~~and~~ that's about what it amounted to. Individuals were selected more for their personal interest than they were by what training they got. I think this is also true in the Navy because I think ~~Zackaryus~~ Zacharias was never as an intelligence officer. He just naturally gravitated into it. So this seemed to be the rule across the board for both the Army and the Navy ~~and~~ certainly none of the sophistication we now find in the State Department and DIA [redacted] and their development of evaluators and recorders with respective ~~to~~ intelligence organizations. It just wasn't that way in those days. And maybe it wasn't needed in those days because the need ~~was~~ wasn't recognized but I'll tell you when it was needed is if we'd had such a force in being and trained like they've got in DIA [redacted] today I think they would have found out a lot more about Pearl Harbor. There just wasn't anybody that knew what the messages meant or had the imagination or experience enough to visualize what the implications of these messages were. So it was kind of an indifferent situation in the sense of training. But as

EO 3.3b(1) OGA

[redacted]

EO 3.3b(1) OGA

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

these new people came in they had to have something to do and they wanted something to work with, and as a few of them learned like Mose Pettigrew out in the Signal Corps did about the existence of this code breaking activity they wanted to see what the Signal Corps and so pressures began to be put on us and some of them who didn't know about it would come in and say, "Well look if you're not reading the German codes we ought to be, you see." And that kind of a pressure was reflected through. Now of course when Pearl Harbor came then the system of priorities got to be quite a bit different, and we got introduced to this early on in the days of our collaboration with the British because one of the things that showed through from our discussions with Dennison and people up at Bletchley Park, Dennison being the one I knew most about because he was responsible for the diplomatic effort down at Barclay St. in London. And some of the people up at Bletchley Park, those who were working on Japanese military and the Japanese diplomatic, well the Japanese military and some of the other Japanese things that I was interested in in my section, became evident that they had to do some kind of sorting out of priorities and requirements, and this was vividly demonstrated when we looked at what happened in terms of the German military solution of the Enigma and a case in point is that the intelligence people would drive real hard to have GCHQ concentrate on its intercept around the Ploesti oil fields, and what was happening in certain areas of Central Europe. While G-2 wanted, as a first order of business at about 3 o'clock in the morning, to pickup a weather report, the old famous Vadsø/Kirkenes (?) from Scandanavia because this message was transmitted all down through

TOP SECRET

middle Europe and it was transmitted first early in the morning up in Scandanavia, so if they got this intercept then they could recover the exact text of the message for that network you see. And then keep pushing it down and finally when they recovered the Central Europe or Southern Europe key then they were able to read all the messages. But if they had tackled only the Southern European intercept it would have taken much longer and been much more difficult job. So you see GCHQ was explaining to us that these kind of problems could originate. I think though so we resolved the problem in a very pragmatic and effective way because Ed ~~Roshour~~ Reischauer Ambassador ~~Roshour~~ Reischauer headed up a small unit of skilled language people who had developed into reporters and had a little cadre of these in what was known as B4, that's the Japanese language group of Arlington Hall Station and then there was this very close interworking. The direct liaison between ~~Roshour~~ Reischauer and his representative and Orell, who was the head of B4, and the mingling together of the translators and intelligence people. All of them knowledgeable in Japanese and so really the problem didn't develop in terms of both Japanese diplomatic and Japanese military. I don't know how the Navy dealt with this, but the German military problem was resolved in the UK theater because thats where the main translation effort was. See we had a group a unit in GCHQ supporting the Bombe effort. This is was Kirby's assignment for example, Roy Johnson, and Bill Bundy was over there in that unit. Bill Bundy was one of the watch officers. That's the Bill Bundy who was Col William P. Bundy's son who was the brother of McGeorge Bundy who wrote STIMPSONS Memoirs REMORSE. Bill was a very very excellent cryptologist, did a bang up job in his assignment there.

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

Well these were the kind of people we had you see so we didn't worry about the translation of German messages. All we worried about was getting Madam X to help out in the solution of some of these situations where there was an important message and its indicator had been lost because old Madam X, the way she worked, she was a relay device, you see, and the Bombe was an analog of the Enigma machine and it had to go through the whole cycle. Madam X could do the cycle bit by piece you see so we could go in anywhere in the message without doing the whole Enigma cycle and get the answer, ~~and we~~ the UK unit could actually select the message that they wanted Madam X to test, put the data in a telegram, radio the code text of this telegram to Arlington Hall Station. It would be decoded. They'd set up the program on the this relay analog of the German Enigma military Enigma (and) would run the test in something less than a half an hour. If they found an answer they'd get the answer back and G2 could run it through the deciphering for this particular message, run it through the deciphering operation and make a translation of it. If they had run the Bombe on it the mechanical Enigma analog they probably wouldn't if they got the answer at all it would have been several hours unless they were lucky. But old Madam X she turned out answers real fast. So you see we really didn't have too much of a sorting out problem because the way the responsibilities developed sort of lead us into a pragmatic, rationalized approach to the problem avoiding any dictatorial actions on the part of G2 as to how we would run our business. I've talked a great deal about the

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

Headquarters operation regarding all stations and a little bit about what the army did in support of the GCHQ which itself is a headquarters operation. Now part of the action which was taken in reference to the total COMINT production picture envisioned what I ~~would~~ like to call as field units. We had a name for them and I've forgotten the name. But George Bicher ~~Beecher~~ for example, who was one of the old students, SIS students and who became a colonel and was assigned to the European theatre early in the war had as his responsibility to develop COMINT support to the field commanders. ~~and~~ We carefully selected officers, reservists and enlisted men and gave them some kind of training at Arlington Hall Station. It was not a very well thought out set of training because we didn't really know what to train~~ing~~ them in. We just made sure they knew what a code was, and cipher was, ~~and~~ what a fractionating system was, because the Germans were using a system that I, just for the purpose of this recording will identify as, I don't even remember the name, but it was a field system and it could be solved. But the best way to solve it was to capture one of the charts

~~Page 7, Side 1~~

TOP SECRET

Tape 6, Side 2 Chart thing it wasn't very sophisticated and I believe it didn't if you had enough traffic it wasn't much of a problem but if you didn't have much traffic if you had just a few messages it would be extremely difficult to deal with and did take some time. Well we envisioned that this is a kind of a system that the field sort of field ciphers of the Germans that the kind of a system they'd use for field ciphers. We thought sort of on the counterpart concept that we ought to be able to read these field systems in the field and give them to the field commanders. Well that was an awful good idea if it had worked but we did find that the field intercept companies provided real good information valuable information but the best way to deal with it was to have a central somewhat remotely located behind-the-lines unit with an increase capability, a rather good capability, rather than two men and a boy and an intercept operator capability. We had to have enough people skilled and backed up with some IBM machines ~~and~~ actually to solve this traffic. And we found the best way to get it done was to send copies of the message to GCHQ where they had a field cipher unit, ~~and~~ when they got the keys they would send them back by secure telegram to the field units where the process then was reduced to a decoding

operation. And that's about the way it worked out. The Germans several times -- and of course the these things were not useful until the invasion had been successfully achieved and then things moved real fast from then on, so the situation changed so fast we never really did firm up on exactly what kind of an organization was best. Now this was a little different in the Pacific and I believe Dr. Sinkov could best answer this question or Hugh Erskine but there was some field activity organized and I'm going to leave that to him because he can tell you the story because he was there and he was responsible ~~for~~, if not for all of it - certainly for part of it, and contributed greatly to what was done in the Pacific. ~~Did that.~~ I think its worthy to note in connection with this field effort that while we were while at least I felt we should be something less than proud of what we were able to do in the cryptanalytic sphere, there was some very useful results produced by what we defined as traffic analysis. Because one, ~~of~~ the techniques of traffic analysis are not so sophisticated as maybe the solution of a double transposition cipher. The information is easy to collect, rapidly compiled, and evaluations and assessments can be made continuously on the data that's been assembled. ~~and~~ In the traffic analytic effort we found that the field installations probably made a probably could do a better job than we could do with any other arrangement. ~~and~~ This of course was directly in support of the intercept operator and in itself was ~~dixxxxxx~~ supported by the intercept activity itself, so there was an immediate and direct interplay of information between the two which in intelligence operations is always advantageous. So I believe that the traffic analytic effort, which the

Americans were involved in in Europe, found its highpoint in the field operation. The question is did we know about the Battle of the Bulge beforehand? This is what I remember about the Battle of the Bulge. It did catch us by surprise, but from the COMINT standpoint there were some messages I think at least one message which carried the key the information about the Battle of the Bulge that did not well resisted Bombe treatment ~~and in after they~~ They didn't realize the importance of this batch of messages because this key message the thing that contained the tip-off to the possibility of the Bulge was buried in this unreadable message. Now in due course this message found its way electrically to Arlington Hall Station where it was run through Madam X, ~~and~~ the answer went back, and in due course the message was translated and fitted in into this other package and when the whole package was tied together as a single package, that is our first clue about the Battle of the Bulge that came out of COMINT. By that time the Battle of the Bulge was on.

End of Side 2

TOP SECRET

Tape 7, Side 1 In meeting the first priorities and also validating the our competence in terms of cryptanalysts, Friedman set us to work on Japanese as the first order of COMINT production business. Yardley's files which had been picked up in New York City when his group was abolished and moved to the G-2 area in the Munitions Building, had been deposited in Room 2742 which was a windowless vault located on the second floor obviously second floor, seventh wing in the Munitions Building. This vault had been turned over by G-2 to the Chief Signal Corps as a storage area for these materials for the purpose of providing background material for this new organization for the Signal Intelligence Service that was being put together. I remember looking into this vault first time we ever knew about its existance, the four of us, three of us really because Hurt was not involved in this particular thing. Friedman told us he was going to take us down to G-2 this morning and to come with him, so we all went down to G-2 thinking it was some important deal, we going to learn something real big, meet some important people, that kind of a thing. He didn't take the time to tell us anything about what we were planning to do, but he goes streaking down the corridors with his natty blue suit and leads us right down to the second floor, down to the seventh wing and right up to this vault door, and when he gets up there he reaches down in his pocket and pulls out a little slip of paper and he twiddles the dial and opens the door, and Then he reaches in another pocket and takes out a key and unlocks the second door and he stands back while this foul air sort of spills out and some fresh air spills in. Then he lights a match, takes a match a box of matches out of his pocket, lights a match

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

and goes in and starts pulling strings, and he pulls on four lights, and Then he goes over and throws two switches and starts two fans circulating with a little bit of dust attended with this last one because this was the dustiest room I ever saw. Friedman turns around and looks at us and says "Welcome, Gentlemen, to the secret archives of the Black Chamber." And that's the first that I ever heard of the Black Chamber. So we got introduced to this. and Then he told us what was in there and he left us for a couple of hours to examine the contents of materials. Once you get familiar with this because this is going to be your basic raw material when we get interested in breaking the codes of other countries. and He pointed out such things as the location of the Japanese diplomatic files, the ADFGVX messages and the correspondence files. and Then told us he'd be back about lunch time and just don't let anybody in but find out all you can about these things. Well this was a real, real goldmine. I tell you there were treasures there. The most exciting things in the world in spite of the dirty, dusty mess. Here were the decodes, the worksheets that Yardley had saved in connection with his Washington conference messages. Here were photographs of things like Spanish codes. Here were letters of commendation from the Secretary of State to Mr. Yardley and his people for the magnificent work they had done and this and that and the other. Here were these old ADFGVX messages. Here were some code books. All sorts of things. You know you just had a ball looking at these things, and We fiddled around down there and first thing you know Friedman was back and says time for lunch gentlemen, and He found us pretty grimy because it was dirty. So we broke off, he locked the doors and I think it was more to excite us than

TOP SECRET

anything else that he let us down there and I think it was a psychological move. Well we went to lunch. We could hardly keep quiet about this. Then we came back to Friedman's office and he laid out the whole ~~list~~ vista of our future for us. This was early on, probably June or July in 1930. Now at this time we there was no activity no work on the Japanese problem at all. But in due course in two or three years we got ready to start work on these old files of Yardley's and this is when Kully and Hurt began an examination of ~~this~~ these materials and we, Abe and I, joined them later along with Clark so we undertook a real positive effort. By this time we were getting intercept from Station One, the one up at Monmouth, and some material on tapes from General ~~Mobern~~ MacArthur -- Colonel Joe sort of down in my basement intercept station and I'm not going to talk about that here but it's a good story for another recording. We soon established how Yardley had solved his codes. We soon established that there were traffic messages intercept of his time which had not been solved and we soon associated the forms of the messages with the intercepts which we were currently receiving. At about this time we also began getting, through some arrangement Friedman worked out with the Navy to which I was not privy in those days, some naval intercept which was of from the Far East diplomatic ~~ness~~ nets that we later identified and which provided unique messages we didn't get from any other source. It was high quality. It was good intercept as ~~ever~~ ever I have seen in my life. Much better than what our teams up at Monmouth had produced and so we had a sizeable batch of material accumulated to work on. Well I'm not

TOP SECRET

going to talk much in detail about how the Japs put together their two- and four-letter codes. That's a separate recording but I would like to deal with the machine ciphers from this point on now that I've laid the background. I would say about 1935 we had all these non-machine systems under control which left a strap of traffic identified by this five digit indicator at the front addressed to GAIMUDAIJIN, Tokyo or the several something like 10 Japanese diplomatic installations Washington, Rome, Tokyo, London, etc, throughout the world and similar traffic going back from these places addressed to well both ways traffic. Now this had resisted our efforts, and we'd done a little playing around with the traffic - this so called five-letter traffic, five digit traffic five digit indicator traffic, that's what we called it and we'd noted certain things in some messages, and this phenomenon seemed to be confined to a ten day period. In some messages we would find six letters would be inordinately high in frequency, with the remaining twenty sort of coming out average frequency for the expected Japanese frequency of appearance for those messages. If you sum the frequency of the six letters which were very high ~~on~~ very low because it could be either high or low you could take the expected frequency of these six letters as a group and it came out that this was the average frequency. This then lead us to another observation. What did the early traffic with these five digit indicators look like, and we found it was strictly ~~all by~~ vowel- consonant and greatly comparable to the vowel-consonant appearance of the Japanese language that we discovered in the mono-alphabetic solution, mono-alphabetic messages that we'd solved, and so we came to the conclusion that the

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

Japs had developed some kind of a way of enciphering the six vowels and the twenty consonants separately so that they retained their vowel and consonant identities and it was reflected through into the cipher text of the message. I think there is a reason for this as I look back because the International Telegraphic Regulations at that time required that a certain number of vowels be present in each five-letter group otherwise it would be charged at a higher rate. So if it was a pronounceable five-letter group you saved money, but if you couldn't pronounce it and it had five consonants for example in the five letter group, it cost you five times as much as five letters. And I think the Japanese had hit upon the trick that if they could have a one-to-one encipherment of vowels to vowels and consonants to consonants they would automatically, because of the way the Japanese language is put together when it was Romanized, come out with a cipher text that would exactly meet the requirements of these international regulations, and they could send five messages for the cost of one. Evidently whoever designed this system had this in mind, because this ~~under~~ was an underlying consideration in their vowel-consonant, consonant-vowel, two-letter four-letter charts you see. The kind of thing that Yardley used under the old LA system which was in effect in Yardley's time and later was found and exploited by us in the early days of our investigation of the Japanese diplomatic traffic and we made a few translations of it. Now the old mono-alphabetic things that I mentioned earlier ~~since were~~ the mono-alphabetic substitutions were designed so that vowels went to vowels and consonants went to consonants. So you got the vowel-consonant relationship in the five-letter groups

TOP SECRET

TOP SECRET

that were transmitted occasionally in this mono-alphabetic systems, so we kind of thought and I'm sure as I look back and give all the evidence that the Japs carried the concept over into the cipher machine simply for the purposes of economy. Well we noted too that the traffic that we started to examine around '35 and '36 had lost this vowel-consonant evidence, and the other evidence that I mentioned namely there would be six high frequency letters and twenty maybe lower in frequency or six noticeably low frequency letters and twenty much higher frequency. We kind of figured that what they'd done was to forget about the vowel-vowel and consonant-consonant relationship and develop some kind of a system that would permit the cross representation of vowels and consonants, and we were simply seeing the effects of this whatever technique and whatever idea or trick they'd used to keep the integrity of the vowel-consonant and pronounceable code group, that they'd gone away from it and indiscriminately mixed the vowels and consonants and were treating them cryptographically as they had previously. Well this as you look at it doesn't mean much but it sort of does prove that there could be two components in whatever system, one dealing with the vowels and the other dealing with the consonants. And that gives you a big leg up on an appreciation of what the Red Machine could be. Well we'd done a little work on some of these earlier vowel messages and I mentioned this morning that this trick that Friedman had used for recovering the wearing of the Hebern wheels, what he called the 066 factor, and we I remember applying this technique to some of those Japanese messages and I remember recovering two sequences, one from a

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

long message and another from another long message on the same day. And the amazing thing about these two sequences which I'd put together statistically and cryptographically is that one was the exact reverse of the other. And it puzzled me and I didn't know what to make of it, and Kully it puzzled him, and Friedman was puzzled but we had other things to do so we forgot about it for a time and I kept it in my junk box and I'll go back and find out why this happened one of these days was my attitude. And then we had this message and I'm up in the 1935, '36, '37 time period. We had this message that excited Col. Bratton about tripartite and we wondered this I believe was one ~~of the~~ those transposed code messages and we wondered what was being said in this unreadable stream of traffic and all of a sudden its importance dawned on us and we put other things aside and we went to work seriously on this. Kully and I did most of the work on it because Abe was away at that time and Hurt was pretty sick and there were a lot of other things to be done so Kully and I did this as a little bit of a part-time job when we had time available to get started on it. ~~and~~ We got our data organized, laid out the attack, sort of figured out what we're going to do not really knowing much more about the system than that it [redacted] had vowels going to vowels and consonants going to consonants. ~~and~~ Then something else had happened and also that as we watched this later traffic where you'd have a high frequency six and twenty letters of lower frequency we could see this phenomenon would be exemplified for a period of ten days. So there were three ten days periods in a month which the frequency phenomenon that I mentioned reflected.

[redacted]

So for example lets take the first ten days it would have a set of six letters be very high. Then precisely at midnight on the 11th of that month this phenomenon would disappear and it would be six other letters either high or low frequency but distinctly different from the outward characteristics of the first ten days traffic. and then if you started on the 21st at midnight the messages could be put in a block that showed an entirely different characteristic for the message content, so it became pretty clear from this evidence which was slowly worked and analyzed over several days, maybe two or three weeks. It finally dawned on us that the Japs were changing their keys every ten days and this was the result of the key change. We also kind of figured each message had a different key because we found repeats only in those messages bearing identical five-digit indicators, ~~two indicators~~. If an indicator was used twice on the same day you might find some repetitions and you'd find a high index of coincidence between the messages when they were directly superimposed. And these pieces of evidence that I mentioned just about the status of our progress on the machine ~~[illegible]~~ when we were suddenly urged to go on and make a big effort on this. Well we worked on it for two or three weeks, sort of ~~started~~ looking for ideas but we hadn't been able to develop anything else of significance other than these things I mentioned. And then Friedman had a conversation with Wenger and he mentioned that we'd been working on this thing and we rather suspected it was a machine and told him a little bit about the sixes and twentys. and this is the time when Wenger described to Friedman the sort of general concept of construction of the

TOP SECRET

Navy machine that the Navy had solved. This is I believe that I'm correct in identifying it as the ~~CONNA~~ KANA machine. I believe that it was the 47 ~~CONNA~~ KANA machine. I'm not sure where I get the term 47 ~~CONNA~~ KANA but it was a ~~CONNA~~ KANA machine and as Wenger described it to Friedman it had two commutators half-Hebr~~ons~~ern which performed a sort of a vigenere substitution on a long sequence and a shorter sequence of ~~CONNA~~ KANA so that the 50 letters of the Japanese alphabet had been divided into two parts somehow or other and then cryptographicly treated, and then the movement of these commutators which were directly linked together by mechanical linkage and could not get out of step with each other was controlled by a motor key which in effect was a 47 tooth gear with a couple of several positions which permitted an extra jump or a double jump of the commutators as the substitution cycle was affected as you went through the message. Well Wenger's discussion with Friedman lead us to lay out the messages sort of on cycles ~~which~~ of 47 and 46 and 45 and 44 and 43 and on down and we began looking for repetitions down columns because Wenger's machine was carried over, the Navy machine was carried over into the diplomatic machine concept then this could be shown if we selected the right kind of letters and the evidence in some cases might be as good as several letters repeated you see. If there was a proper repeat in the plaintext this would be reflected in the cipher text. Unfortunately we found nothing like this, ~~and~~ so we milled around for quite a while trying to resolve this machine concept we'd developed for the system we were attacking based on what Wenger told Friedman. Well at this point we sort of stepped back and took a look at where we were going and see if

Wrong ("Go-on" simply refers to the pronunciation of a Chinese character as coming from the old Chinese pronunciation of GO. WARNING (in contrast with Kan-on" where the pronunciation derives from the old Chinese pronunciation of Kan)

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

we couldn't devise some other approach that would offer us more hope. We did a little bit of a tentative survey of what of the cipher machines we knew about, for example there was this DAMM machine that I mentioned in other recordings, there was our own M134, there was our own concept of the ECM that was now in the process of being developed, a German Enigma, the Hagelin machine and whatever the Kryha and whatever other machines we could think of we said are there any characteristics of these machines that would show this vowel to vowel kind of thing or the high frequency, low frequency six as opposed to the different frequency for the twenties and just what is there, and we found nothing that equated to a that would enable us to produce the phenomenon that were very evident now. So we obviously had to come to the conclusion that this was a cipher machine, and the evidence was pretty good that it was because what the Navy reported and what we had found out, that it was an entirely different kind of cipher machine from anything except this Navy machine, and it had to be different from that because the Navy machine had a much longer a greater capacity the 47 50 go-on that comprise the Japanese written alphabet because this was limited just to the 26 English letters so there was a modification of this Navy machine and significant modification probably. Well we didn't quite understand all this and the Navy didn't give us any more details, so I guess Wenger went just a little bit further than he thought he was authorized because Friedman didn't see him for quite some time. Well sort of in desperation Kully and I one day after lunch thought we'd go back and look at these early messages worksheets that I'd done some earlier work on and because I felt real strongly that if you carry the

TOP SECRET

bull when its a calf ~~but~~ that you may carry it when it's grown. I kind of felt that was a good philosophy even though it was pragmatically not so in the case of the example. So I persuaded Kully maybe that we ought to go back and get these old messages and work on them and I think it was a pretty good proposal because we began to imagine how we could ~~get~~ guess some text you see. We sort of looked at these monoalphabetic substitutions to see what kind of words were in it and one of the things that hit us was the word ~~OYOBE~~ "OyoBi" which was three vowels a consonant and a vowel you see. And that was a kind of odd pattern. You can develop this like if you have a double KYUU~~key~~ for example you get this pattern but ~~OYOBE~~ OyoBi is a very frequent word and these other patterns produced this kind of thing are somewhat less frequent. You have to say "and" in all languages and ~~OYOBE~~ Oyobi meant "and". Well, we wrote out some worksheets and we started looking for ~~some~~ patterns. We found a lot of interesting things. We found sequences of where the vowel consonant pattern for several letters would match the vowel consonant pattern in other parts of the message which lead us to believe these might be repetitions. We also found a lot of possible ~~OYOBEs~~ OyoBis. ~~and~~ Then we thought what other things could we use. There was such things as TOKORO, KOTO, KOTO TO NARI -- the Japanese language has got a lot of grammatical pecularities where they have to use a lot more letters to take care of such things as is represented in English by "has" and "have been" and the subjunctives and other things that all have the peculiar ways ~~of saying them~~ of representing these thoughts, ~~and~~ so there were certain combinations of words that were most frequently, well unduly frequently as you compared ~~it~~ with the "have" and "has" in English so we started looking for these things. Finally we patched together enough possible so we thought we might start to do

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

something with it. Well the reason we wanted ~~OYOBE~~ OYOBi is because that gives the chance to develop some kind of recovery of this six letter sequence because you see with five letters, four of them being vowels sort of went along with each other if we could get some of these hanging together than we might produce the six letter sequence. Well there was one message one of the long messages we had. We soon began to get some letters hanging together and finally we got a total compatible group of six letters which applied in several cases if we used those six letters. And we couldn't go much further than that because we didn't hardly see how it would work. So ~~in~~ sort of catching our breath we compared this sequence with the two statistically produced sequences and lo and behold it was identical with one of the sequences been recovered by the statistical method ~~and~~ We felt real good about that because we felt that this this was a significant assortment of letters and we ought to be able to get something out of it. So we went to the cases ~~of~~ for example ~~OYOBE~~ OYOBi where we found these six letters hanging together and we began assuming these were ~~OYOBEs.~~ OYOBis. We didn't have enough sort of to lay the thing try to break the solution bring the solution into full being. So we had to back off and said well now we'll have to deal with the twenties. How can we recover these? And ~~I reckon~~ by making certain several assumptions and doing some guessing finally we developed some plausible plaintext. I believe MANSHŪKOKU -- since this was a Far Eastern message was a good candidate and I seem to remember one of the guesses we made was the romanized word for Manchuria and a couple of other

TOP SECRET

TOP SECRET

things, these TOKORO, KOTO NARIs were useful. and so on and Finally we began to develop about ten or fifteen of the consonants which seemed to hang together and to get some plaintext, and then for some reasons all of a sudden things jelled. I don't remember just how they jelled but we were operating these two sequences the six and this tentatively recovered twenty sequence just like two Kryha sequences you see operating in synchronization. When we found a vowel we would decipher it with a vowel six sequence and when we found a consonant we'd move both of them one position because it had to be one position the way the two things had been put together, and decipher that and pretty soon we were getting little patches of Japanese plaintext that looked real promising. and Then we'd make a guess or two and first next thing you know we had the sequence put together. But every now and then as we'd go through the message we'd find the thing got out of sync and sometimes we had to step it two and occasion three positions instead of one, but we'd go for long stretches before we had to make this extra jump. Well we sort of stopped and looked at this thing and then we found the most promising place and we decided we'd work back and forth from this particular point and putting in the plaintext it seemed firm using the sequences we'd recovered and then see what would happen. And I remember we were both working together. I was manipulating the sequences. Kully was calling the shots from the worksheets you see and both of us would check what resulted. He did the recording and I did the manipulation, and we both evaluated the results of the application of these two processes, and we found that by being very careful and

TOP SECRET

TOP SECRET

selective we could produce about 50 or 60 letters of plaintext if we allowed ourselves to take some extra jumps somewhere in that stretch. And then we kept pushing it and finally when we got down to about 120-125 letters, Kully was making red marks on the sheet of paper with a red pencil where this extra jump came in and we began to count the intervals between it and lo and behold it came out to be something like 43 or 44 which was in the ballpark of the 47-tooth wheel that Wenger had described, and I think we knew we were over the hump at that point because then we began to lay out these red marks in advance and going backwards, you see, and seeing if we'd adjust the sequences just what would happen and lo and behold these sequences and through this sort of cut and try operation keeping in account this 44 cycle did produce a decode, a logical clearly Romanized Japanese decodement of this message. We didn't worry about what it was saying. We just worried was it good Japanese and could we produce more of this. Well by this time everybody had gone home but Kully and me and we were tired and it was almost, well it was pretty late in the afternoon, It was about 6 o'clock and we felt good and we felt tired. We decided we'd lock up and go home and come back in the morning and take it from there and we did. We came in the next morning. Both of us got there real early. We just couldn't wait to get ahold of this. Fortunately we worked behind this steel door, you see, and we could leave our papers and everything on the table, just walk up and lock the door leave them, and come back next morning and we didn't have to look for a thing. We didn't lose anything. We didn't have anything in our way, so

TOP SECRET

TOP SECRET

we just went ahead, sat down and carried on. Well Friedman didn't come in on time that morning but the rest of the staff came in and we were so busy they didn't pay much attention to them and we were so anxious to really make sure that we knew what we were doing that we didn't bother them much and so we decided to go on and try the other message. We tried the same trick, scooting the wheels the same way we did in the first message. We didn't get a thing. Then it dawned on us that maybe if we slip them backwards instead of forwards and follow something like this pattern we might get text, and lo and behold we did. And lo and behold this was the reverse of the sequence because the simplification statistically that we had noted earlier now became a real thing because you could get this reversal of the sequence by sliding the two components in the opposite direction, so we figured the machine then had to consist of something like this: Two half Hebern commutators, the one accommodating six letters and the other twenty which were rigidly linked together maybe on a common shaft, and these were motivated either forward or backward by a motor wheel which basically had 47 points or 47 teeth if you will with provision made for interruption. We also noted in the second message there was a different interruption pattern from this motor wheel than we found in the first message. So we had pretty good evidence since we had plaintext in two messages. One by pushing the machine forward and the other by pushing the commutators backwards that we were into the machine and we were substantially close to a total solution of it. The only thing was how now to read message number three. Well by this time Friedman had come

TALENT KEYHOLE CHANNELS ONLY

TOP SECRET

in and we couldn't wait to tell him and he came in and ohhed and awwed sort with us and said "Gee, we're real proud of this because here now we going to read all these other messages that hadn't been read for years." And indeed it was years because the machine went into effect in 1932 and this was up in the towards the late 40's, I mean the late 30's early 40's pretty close to 1940. Well Friedman thought it would be a good idea if we got the other people into this thing because a lot of work to be done and we wanted to get right on with it you know. Everything was hot and fresh and piping and so we organized our effort. We thought it would be a good idea to do a little more work on this batch of old messages to see what else we could learn because we knew the sequences and it was easier to deal with it, but we were very anxious to get down to some of the Washington-Tokyo messages which had been currently intercepted and which we'd done some work on where we knew the frequencies because quite clear now to us that what they'd done was to mix the vowels and consonants in the subsequent and current traffic. Well we -- Kully and I since we were familiar with the techniques involved in our study of the Red Machine package continued to try to read some other messages and we read three or four. Meanwhile Clarke and Mrs. Nelson, Louise Newkirk was her maiden name, and some others of the staff began to set up worksheets which we thought would be advantageous in our analysis of the current traffic and we specified of course now it became evident that the ten day statistical evidence was really significant and we specified that we would use only messages which showed this characteristic of high six letters and hopefully we would

find one with the two vowels in the sixes because then we could use this 066 phenomenon to recover the six sequence and then we'd use it as a penetration into the twenties, and thereby the Japs in their lack of appreciation of just exactly what they were doing by dividing the sequence into two portions, one a six and one a twenty, had given us a cryptanalytic handhold into their system which they would have avoided had they not done it. Without going into the details of how we managed to apply the techniques that had been developed in our initial break into the system, before the end of the day we had forced out the text of a couple of the current messages and had determined that in effect the basic structure of the machine had not been changed, only the manner of its use namely that the vowels and consonants had been intermingled instead of kept separate as they had been in the messages which we had read the day before. We also verified that the sequences which we had recovered for the current messages remained in effect for a period of ten days and that there were a variety of interrupter patterns, evidently associated with some kind of an adjustment that could be made on the 47th tooth wheel which... This effect was then transmitted to the substitution component in the machine so that we found that we could simply decipher the messages using a Vigenere effect and allowing for the interrupter patterns and duplicate the operation of the machine with cross section paper and a properly prepared worksheet which would enable us to keep track of the location of the sequences, their position with reference to the 47- tooth wheel and the position of the 47-tooth wheel itself. We also imagined at this point in time in that there was a plug board somewhere

between the commutators and the keyboard printer mechanism which the machine evidently employed and we weren't sure that this was a mechanical printer mechanism like you'd find with an electromatic typewriter with solenoids or a lank bank arrangement we found in the first model of the Hebern and the Enigma and in the Hagelin the Damm machine which had been built in Sweden. It was also evident that there was some kind of a gearing arrangement which would permit the motor wheel to drive the commutators operating in synchronization either forward or backwards. This was in effect the direct/reverse sequence that we had found employed both in the earlier messages that we had solved the day before and in the messages which had been forced out which were of current intercept date. The next couple of weeks putting our work on the Red Machine traffic we did not call it Red Machine in that time frame we just called it the Japanese cipher machine because that was the only one we knew about. The work on the Japanese cipher machine then was given high priority during the next few days and we tried and recover and force out as many keys and messages as we could and finally we reduced the whole process to a rather simple, straightforward crypt-analytic exploitation process. We found that the keys remain in effect for ten days. That each indicator appearing as the first group of the message that is the five digit group identified the starting position of the two sequences the six and the twenty sequence, identified the starting position of the 47-tooth wheel, and as I recall the interrupter pattern which had been set up on the wheel remained in effect for a full day, and it was only what point of the 47-tooth wheel that was to be used as the starting point for the first letters of the message. --

This was the only change in the motor wheel application. Without going into further detail on what we recovered and what the machine looked like and how it operated I believe it would be better to examine this in terms of the videotape which is planned then to continue trying to describe it verbally. As soon as it became evident to Friedman that we had actually and successfully penetrated the Red cipher machine and that there was no reason that we could not exploit it fully, he called in the Chief Signal Officer and our immediate boss, the ~~head~~ chief of War Plans and Training Division, and explained what had happened and showed them the text and needless to say they were real delighted and somewhat excited because here was evidence of the payoff off on the sort of long-term investment that the Chief Signal Officer some years before had undertaken. The next step of course was to apprise ~~G2~~ G-2 and its interesting to note that Friedman and Chief Signal Officer and Chief of the War Plans and Training Division had some reservation about this not because they did not trust ~~G2~~ G-2 but because they were afraid ~~G2~~ G-2 might be so anxious to have us start delivering productive translations that we'd not be able to carry on the research which they felt was necessary to complete the other missions that had been planned for the Signal Intelligence Service. So I suppose it was with little trepidation, not a great deal, but they made the decision to apprise ~~G2~~ G-2 folks of what had happened. The Chief Signal Officer did this by calling on the Director of Military Intelligence whose name I have forgotten now and in a couple of days we had two visitors, Col Bratton, who was on the Japanese desk, and I believe one other officer from ~~G2~~ G-2 and they were indeed pleased and delighted to see

TOP SECRET

what kind of information was contained in the few messages that Hurt had been able to translate. Bratton was particularly excited about the break through because he had never before seen such a complete and authentic text. He had some doubts about Mr. Hurt's code recovery ability but there was no question that the romanized text was exactly the Japanese that had been transmitted and there was no latitude for ambiquity in the text produced by the decipherment of the Japanese cipher machine message. He was also somewhat amazed how carefully the Japs worked out the romanization so that in cases where the Romaji representation might not have been clearly defined they had taken other steps to clarify the text. In our discussions which took place after we made our demonstration Friedman raised the point that there was still a lot of work to be done, there was a lot of back traffic to be read and we needed to recover more information about the indicators which at this point in time had not been solved and suggested that it would be better to clean up the solution activities before we went into full production on the current intercept traffic. Bratton ~~Batton~~ was pleased about this suggestion because he wanted to personally examine the Romaji text resulting from our ~~decode~~ decipherments of the messages because he felt there was such a volume of them that he did not want to be burdened with numerous translations of low interest, but would like to determine what categories of subject matter would be of most use to G-2 thereby conserving both his time and Mr. Hurt's time. The Red machine did in fact seem to carry the bulk of the high level Japanese

TOP SECRET CHANNELS ONLY

TOP SECRET

foreign office correspondence between Tokyo and the outlying stations which the distribution was made and these as I recall were Washington, London, Paris, Rome, Berlin, Moscow, Ankara, Warsaw and a couple of and the headquarters of the Far Eastern diplomatic net. I believe this allows for ten including Tokyo. Ten links. We also found that in some cases there would be book messages going to two or more stations and if these two stations held the Red Machine they always went in the Red Machine. If one of the stations to which the book message was addressed, maybe Mexico City for example, then the Red Machine would not be used for that message, but one of the codes held by Mexico City would be used and usually ~~if~~ it was the codes which the manual code the two-and four-letter code that was used for this transposition, a rather simple transposition-superencipherment. So we felt that we had really tapped the main high level stream of Japanese foreign office communications and we had successfully broken this Red Machine. It remained in effect for several years after we'd achieved after we'd been successful in solving it. ~~and~~ Its replacement machine which came in in March 1939 did not fully replace it, but some few messages for several months after March 1939 continued to be sent in the Red Machine. We also found that in some installations the machines were not operating effectively. One machine, and I don't remember which capital it was, had a fault and it kept generating garbles in the message both for the Japanese and ourselves and ourselves until we found out what caused the garbles and then it quit bothering us, but the Japs never did learn and so they asked for several resends. ~~and~~ This amused us and made us feel pretty good. We really felt smart.

~~TOP SECRET~~

Smarter than the Japanese and I suppose justifiably so. Now probably the next significant development in connection with the Purple machine was that after we'd been reading the messages for several months we discovered there was a pattern to the formation of the sequences ~~of~~ the six and twenty sequences and we began to develop new sequences which we'd find repeated elsewhere which we could find appearing elsewhere although in a different form, but we could predict and generate ~~these~~ a whole body of sequences, and finally we got enough information together so we could actually predict and identify for several months in advance what sequence would be used and what the date period for the sequence would be when the Japs put it into effect. Also another significant development was that the Japs stopped their ten-day change and went into a daily change of key and finally it turned out that the exploitation of the Japanese Red cipher machine traffic was probably the easiest task we had in front of us at that time because it was so automatic. We also undertaken to build an automatic machine which we asked the Navy Department to construct, and as an interim deciphering arrangement we constructed I think I built some of these in my basement. We constructed little cipher devices like the cipher disk like the old Army Signal Corps cipher disk except modified and arranged so that we could write in the sequences in pencil decipher the message and by keeping track of the interrupter pattern actually decipher the message rapidly by the use of this little celluloid disk. Now there was a little bit of a question about whether or not, right after the system had been solved, whether we should tell the Navy about it. But I don't think there was

~~TOP SECRET~~

much of a problem about ~~finding~~ making the decision to tell the Navy because it became clear that what Wenger had told us about the Navy machine had been useful in working out the principles of the Red Machine and we felt maybe this information would be useful, I mean similar information from our work on the Red Machine would be useful to ~~be~~ the Navy in some other aspects of naval cryptanalysis on Japanese naval systems. I think this principle was a good one for us to follow and probably the ~~worse~~ worst effect from it was that the Navy found the information so valuable which is contained in these Red messages, that they decided they should undertake likewise the exploitation of the Red traffic, ~~and~~ This offered no problems on the technical level because we fully coordinated our technical work to recover the sequences, and it was from this arrangement we were able to ask the Navy to build the automatic cipher machine keyboard operated with a printer. The problem though which developed came out of the fact that when the Navy translators would find an interesting message they would go ahead and translate it without reference to the Army and similarly we in the Army would make a translation if we found this message of interest to ~~G2. and~~ G-2 Then sometimes -- in the few people who were privy to the fact that we had read these messages sometimes they would be confronted with two translations sometimes almost identical but in some cases different enough to raise questions about the validity of either the Army translations or the Navy translations and this caused some problems. Also another problem developed in connection with discrepancies between the translation because ~~the~~ as soon as the information the contents of these messages

[redacted]

had to be disseminated out of the War Department (and) Navy Department, say to for example, the State Department, and they were of considerable interest to certain State Department desks, then the question of who got the credit for the production of intelligence raised its head because pretty soon G-2 and ONI when they got a hot item would start running up to the State Department authorized recipient and they would both flip down these somewhat different translations in some cases and then raise a lot of questions and this problem got up on a pretty high level in the Army, Navy and again if I can in a lighter vein refer to the General/Admiral syndrome of competition some kind of a split had to be determined. Some way of avoiding duplication and each side getting the fair share of the credit. Those of us in the Army felt like well we'd actually broken this machine. Our people ought to get all the credit for it you see, and the Navy on the other hand felt like well intelligence is intelligence and if we find some we think is interesting there's no reason why we shouldn't produce it and go up there, so there was pretty good basis on each side, and finally some one proposed the solution that if the Army took them up on the odd days and the Navy took them up on the even days, and then this does sort of smack of gasoline rationing today that this dilemma would be avoided. Actually this initial solution was a very poor one because the date of translation was used as the identifying date and the Army might translate a message on the first of January for example and the Navy not translate the message until the second and then you still had the duplicative evidence and problem ahead of us.

[redacted]

[redacted]

TOP SECRET

Tape 7, Side 2

Finally we resolved this problem by using the cryptographic date of the message because the Japs were now changing the keys, the sequences on a daily basis, ~~and messag~~ If we could identify the sequences used, for example, ~~used~~ on the first of January, every message using this sequence then automatically became a first of January message and consequently an odd day. If the sequence for the second day of January was used then this message was an even day, and we actually put the onus of selecting the date on the Japanese originator of the message in the code room clerk when they put it in the machine using the sequence of the day.

TOP SECRET

Tape 8, Side 1

TOP SECRET

Q As you choose. I think you can pick it right up with the beginning there if you wanted to or as you and Kully and Abe Sinkov became, got into it, and as it started to grow.

A: Well I think we have to go back to the very early days of the Signal Intelligence Service. As is pretty well documented, Yardley's operations conducted in New York City was the only cryptologic operation of any importance that had been developed in the U.S. history. It had its genesis in the WWI requirements and Yardley carried on his staff which had been developed in WWI through the 1920s [up ~~through~~ until 1929 when Secretary of State Stimpson decided that this was unappropriate thing for the State Department to be associated with. When Yardley's organization was actually abolished by Stimpson's, I'll call it a decree, because I can't think of any other word that describes it better, a need was recognized for this kind of intelligence.] The reason the ~~G2~~ G-2 probably the reason the ~~G2~~ G-2 became aware of this was because they had been funding part of the Yardley operation and when the Black Chamber in New York City was abolished they had these funds available. ~~It~~ There was also considerable evidence and full realizatio the importance of of this evidence that U.S. systems had to be improved. At that time the most popular form of cryptography was a great big two-part code, something like 60 to 100,000

DoS

over in G-2

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

groups and these were expensive things. There were no machines to eliminate the burden of encoding and decoding, but these codes, the big two-part codes, were expensive things and they would last only as long as the security was maintained either through second-story compromise or cryptanalytic compromise. In those days sort of second-story or surreptitious entry aspect of compromise was much easier to achieve than it is today because people just weren't security conscious, so you, it was kind of figured by G-2 and the Chief Signal Officer, who was responsible for the part of the code production program, that some improvement had to be achieved. Also at that time the cryptographic process, the encoding process was separate and apart from G-2 and Chief Signal Officer and was the responsibility of the Adjutant General, so there was a sort of three-prong direction/administration of the cryptologic effort. G-2 was security, Chief Signal Officer for the technical aspects of code compilation and the transmission of the messages, because the Chief Signal Officer was running the War Department networks and the Adjutant General and his responsibility for keeping the records and conducting the correspondence of the Army or the War Department as it was known at that time. Now this sort of mishmash--lack of any single line of responsibility plus the general

TOP SECRET

uncertainty about security made G-2 and the Chief Signal Officer extremely nervous and there was also the requirement of intelligence, production of intelligence by cryptanalysis, that they looked on as a sort of longer term arrangement. But they had to get some kind of a force into being because Yardley's force had been dispersed and at that time they decided the Chief Signal Officer and the Director of Military Intelligence they would take this ten grand and build up a new organization, and they had a real good foundation for this because Billy Friedman had been hired by the Chief Signal Officer some five or six years before in the middle '20s to supervise as a sort of one-man effort the production of codes for the War Department and they decided to augment Friedman's staff with a small unit hopefully four people who would be trained in all that was known about cryptology which in essence was all that Friedman knew because that was the only source of information anywhere in the world that was available. Other countries maybe Britain might have known more, but Friedman was the only one who could be contacted or utilized by the U.S. government, so Billy was given the job of selecting four fellows and hiring them and his administrative responsibility was to determine two things initially followed by these other things. The two things was what type of people he needed and what

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

kind of training they needed and that administrative problem was pretty simple because the funds available were only enough to hire about four people and he pretty wisely selected mathematically trained people, individuals with college majors in mathematics and he hoped to supplement this mathematical background with some linguistic background and he had in mind four languages; French, Spanish, Japanese, and German. So Well this selection is based on mathematical plus. An individual with some competence in each one of these languages. To get a little bit off the sort of administrative pattern and talk about the reality of the situation, he was able to find three mathematically trained people with the desired languages French, Spanish and German. Abe Sinkov was the French speaker, Kully was the Spanish speaker and I was the selected because I'd had a couple years of German in college but he couldn't find a fourth with mathematical training who knew Japanese. So he had to stop with three and later on we were extremely fortunate in getting a fourth, Johnny Hurt whose ability with mathematics was anything but striking. He never could add two and two twice in a row and get the same answer and he wasn't ashamed of it either thank God.

I suppose I should explain why Yardley or members of his staff were not involved in this regeneration of the cryptologic effort, but the simple fact is that the

TOP SECRET

Director of Intelligence and Chief Signal Officer was afraid that if the Secretary of State found out that they had planned and were undertaking the regeneration of the cryptologic activity ultimately aimed at doing exactly the same kind of things or performing the same mission for intelligence purposes that Yardley's organization had performed, that steps would be taken by Stimpson's organization, the State Department and his staff, to get a Presidential edict which would completely eliminate any hope of regenerating this kind of effort, so feeling that Yardley or any of his people being employed for this kind of purpose might put off the fact that steps were being taken to regenerate the effort to the State Department with the consequence it would be abolished lead them to avoid Yardley and his people as if they were not Americans. Now what was happening in other places? Very little. If you'll read Yardley's book you'll find that the Navy's attitude towards the intelligence production through cryptanalysis was either unknown to him or somewhat indifferent, and as far as I was able to learn after I came in in 1930, the Navy's effort was inconsequential. The State Department of course had been bled by Yardley for anybody with any skills of this nature in setting up his organization and there wasn't anybody else. The Bureau hadn't of course had not come

into existance in those days. Whatever little law enforcement there was was probably left only to the Coast Guard and its efforts in apprehending rum runners as a result of the prohibition laws, and incidentally in that area there was an effort which was Mrs. Friedman's effort. She as Billy's wife had been trained in Riverbank Laboratories. That's where they met and got married, and she was running a small cryptanalytic bureau as a part of the law enforcement operations of the U.S. government, and as I look back on the use of the information from Mrs. Friedman's unit, it was intended to be supplied to the courts in the prosecution of these violators of the Prohibition Act and it was forcing into the press and into the news media the capabilities of the Coast Guard in this field, which would be intolerable under today's -- at least under the classical concept of security. Of course after a while when prohibition was removed from the laws there was no need for this unit and some of the people from the unit joined the later on activities of the Signal Intelligence Service.

After we had been assembled and Friedman has started us into our training program, the next phase in the development of U.S. cryptography became apparent and that was the adoption of an improved systems over and above these

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

antediluvian two-part codes that we were then employing. Friedman had a conviction that the mechanization of the encoding and decoding process was the best answer for the times for the problems of the U.S. government and he had dedicated himself to the development of cipher machines. He had collected and studied all the cipher machines that could be purchased on the open market at that time there was not enough second-story work to give us an insight into what other nations were using but it was pretty evident from Yardley's files that no other nation was using anything except some form of code book and some of these were enciphered and others were just big two-part books. Well Friedman's dedication to this lead to the Signal Corps launching on a research and development program to produce a cipher machine and other forms of cipher machines for the ultimate cryptography of the US War Department. This was part of the management in the sense that we were pushing forward the frontiers of the unknown in cryptology to embrace improved systems and faster means of performing the coderoom process because using a two-part code is a time consuming and error producing operation, to digress a minute I spent some weeks in the War Department coderoom as part of my early training and one old gentlemen there, a Mr. Williams who was about ready to retire, had memorized the most frequent groups in the code and he

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

was the fastest code decode operator I ever saw in my life, But he just produced the answers out of his memory and it was only an infrequent group that he would have to look up in the code book, and he would sit at his typewriter and take a copy of the message from the Western Union or the Signal Corps Telegraph operator and actually write out the plain language just like somebody who was skilled in German could translate a German message into English. But this required many months of training and a particular apptitude on the part of the individual so Friedman's way of beating it was to develop cipher machines. Now the next phase in the operation of the Signal Intelligence Service was to complete the basic training in all aspects of cryptology including the principles of how to solve the known cipher machines that Friedman had developed, and when we completed this part we then embraced embarked on the code compilation program that had been laid out by the Chief Signal Officer and this was quite an administrative problem because it involved the production of these large code books. There were two or three editions of the War Department staff code which had about 60,000 groups. The and that was two-part, and that was a very onerous job because each group of each section had to be individually cross checked against

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

every other group of every other section. It was just like climbing a million mile mountain to compile one of those things. You never get to the top so it seemed to us who were doing the proofreading and checking. In addition to these two very important codes there were other codes, War Department staff codes, War Department confidential code, and a great number of army field codes and division field codes. Now probably one of the most important management decisions so far as cryptology is concerned was taken just about that time and that was to rent IBM equipment to assist the cryptologist in their code production program because the IBM equipment in those days the accounting machine equipment, which consisted mainly of key punches using cards and sorters and reproducers and printers, were ideal for the code production program and when this step was taken and we proved that it was a good step to take, I say we because Friedman and his staff were the ones who actually did the work of showing how these could be applied. We produced a whole series of division field codes, a two-part code, ten thousand groups in less time than normally it would take to produce one code and then and it could generate other codes after we'd done this first batch we could generate other codes in something less than the 25th or the 30th of the manhours required by the previous techniques. Now this

management problem and its early solution certainly encouraged Friedman in his philosophy of mechanizing as far as possible the cryptologic process. ~~and~~ It carried it into the earlier stages of cryptography rather than just the code room which is the "use" stages as I look on it in my concept of the flow chart. He got back into the production stage and really the preproduction stage. This was where we could develop the vocabularies that would be required for each one of the varieties of codes. For example, the vocabulary for a code at division level is entirely different from that at army level and quite another thing from the one we used at the department level which would ~~could~~ be the Secretary of War in those days and the commanders of the corps areas in the overseas departments. Now this training program and the early operations on the code production program occupied our attention for the first four or five years of our effort probably more than anything else. But during this time a separate activity was being undertaken as part of the cryptologic effort of the War Department and that was the development of the intercept or collection service. ~~and~~ This is pretty well defined by the Second Signal Service Company activities if you go back into history. We'd planned several intercept stations the first of which was to be at Fort Hancock New Jersey, close to Fort Monmouth, and another one in

Washington, and ~~then there~~ were three in the overseas departments, and one at the ~~Psidio~~ Presidio in San Francisco. We though t this would be I say WE I'm talking now collectively about the people who were involved, but mainly this was the Chief Signal Officer and the Director of Intelligence -- thought that the ~~would be~~ would be proper arrangement to have these collection activities located strategically throughout the world where they were under control of US military installations. ~~The~~ Once these collection activities began producing intercepts and ~~G2~~ (G-2) took note of this then ~~G2~~ (G-2) generated another kind of an administrative problem. When Mr. Chief Signal Officer are you going to start producing intelligence from these things? You've got these boys, you've got the ten grand, Friedman's got them just about trained, how about some decodes? And so this lead us early on to tackling our first foreign government code system. In those days there were these priorities: Japan was the highest, Germany was second, and Italy was third, and I've just defined the tripartite organization which was the obvious threat to US security that appeared on the horizon at that time. Then everything else was sort of lumped together. Well the administrative problem involved here was to transform our somewhat theoretical training more directed at the production of codes and the satisfaction of the code production requirements than intelligenc

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

~~SECRET~~

requirements into an activity which would produce decodes of Japanese messages for example. ~~and~~ Of course with Japan being our highest priority and with the Second Signal Service producing intercept Japanese diplomatic messages, we naturally fell to work on the Japanese diplomatic systems. Yardley had done in his group, had done a very commendable job on this. You can read in Yardley's book the story of the Naval Conference success -- ~~was remarkably in favor~~ it was a real noteworthy cryptanalytic achievement for US intelligence, ~~and~~ so ~~we~~ Friedman's idea which was endorsed by the Chief Signal Officer and the Director of Intelligence was to capitalize on the basic work Yardley had done and try to advance it into other work on the Japanese. So we picked up the thread ~~and~~ about 1933 examining Yardley's files learning all we could from them, and tackling the current intercepts. Now one of the things that had to be accomplished was to develop enough knowledge in the cryptanalytic force of the Japanese language so we could break the ~~diplomatic~~ codes involved. So part of our training program was directed then to that being introduced to the Japanese language which was a terrible thing for an American to learn in those days. Fortunately we had one real good expert. That was Johnny Hurt. He and his knowledge of the language

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

TOP SECRET

got us over the gap. Hurt unfortunately contracted tuberculosis and we had to use some other instruction. This kind of amuses me as I look back on it because we hired a white Russian who was a part-time employee of G-2 and who had studied Japanese when he was in the Russian army, he was a colonel in the White Russian army. He studied Japanese at the Oriental Institute in Moscow and his English was atrocious and sometimes the only way I could tell what the man was trying to convey to us in English was to ask him in German which he spoke fluently or for Abe to try him out in French, and after about three or four months of this we finally gave up and went back to self-study and we did a lot better with self-study than this white Russian colonel. Incidentally his name was Colonel AVASAGU(?) and I don't know how to spell it but we used to make jokes about the colonel and his AVASAGU Now with the generation of the effort on the Japanese it took us a little while to get to make a break into the current code. The Japanese had changed their codes save for one. This was a code which bore the indicator two digit indicator LA and had been used in slightly different form and had been solved by Yardley, and I might just give you an idea about the life of this code by saying that in the end of WWII when the Japs sent the surrender message from Tokyo to Berne they used a more modern form, an updated form of this same basic code which had not been changed

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

so far as the more frequent groups had been concerned, but we had this to get started with. ~~And~~ It was a wonderful thing. It sounds like a stupid thing to try to read the most, the least secure code of a nation, but from our standpoint we developed a great deal of important statistical information about the Japanese language as it appeared in these telegrams, ~~and~~ I might point out, the diplomatic, the frequencies of diplomatic language is somewhat different from newspaper frequencies and it's important to know and understand and appreciate this which we soon did from our work on the Japanese. It also gave us a feeling for the type of information that would be contained in the messages because there ~~it~~ would be cross references and we could understand particularly something about the Japanese financial ~~columns~~ problems and the traveling of staff people ~~and~~ in the Japanese foreign office and other things like that. Now we, early on of course, and I'll brag a little bit here, we early on got into the business of reading some of the ~~cipher~~ simpler codes that the Japanese had employed and this as soon as we had recovered enough of the groups to produce skeleton translations or gist translations we would turn these over to ~~G2~~ G-2 ~~and~~ Colonel Bratton, who was then the head of the desk in ~~G2~~ G-2, would come up and sort of discuss with Hurt the text of the messages he was working on and ~~it~~ there was a sort of crossfeed, and this is important

~~HANDLE VIA COMINT CHANNELS ONLY~~

TOP SECRET

from an administrative standpoint to appreciate. A crossfeed from the people who have requirements for intelligence by cryptanalysis or communications intelligence with the producers of it to feed in the collateral information which is essential to update the producers with the realities of the intelligence world. Now this is more or less automatic in the present day concept of NSA, but it basically satisfies the same requirement of updating the knowledge of the people who are trying to break codes with the kind of things that are being discussed and with the details of what is discussed. ~~and~~ What we're seeing in this present day organization of feedback between the intelligence agencies and our own massive information files here is the outgrowth of this very simple impulse which wasn't invented really by Col. Bratton and Johnny Hurt, but which was a natural consequence of the kind of work that was being done. An interesting aspect of our work early work on the Japanese codes was that these skeleton translations and some times full translations because when we'd worked enough on the code to get it fully recovered Hurt could turn out a real good translation of these things, wetted Col Bratton and his staff's appetite for more intelligence and one of the things which was right on the top burner of the stove at that time was for ~~G2~~ G-2 to find out what they could about the arrangements

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~TOP SECRET~~

TOP SECRET

among Japan, Germany and Italy in terms of this tripartite alliance which was brewing then at pretty much of a fever heat and which really looked like the most ominous cloud on the US future. One day Hurt had turned out a message -- translation which was not very complete. It was more or less a skeletal thing. This was a very odd message. A circular message that had been transmitted from Tokyo to the more important posts and stations throughout the world... Japanese foreign office posts and stations, and It had a very funny -- not funny but a unusual beginning. It started out with a Japanese phrase " KANCHŌ FUGŌ ATSUKAI ~~to~~ which literally translated means "For Officials Eyes Only," or the German had another one "To be Decoded by Officers Only" and this tagged it as an important message. Well Hurt worked this over pretty well, but the code was not sufficiently recovered for him turn out much more than just the bare gist of what the message was about. ~~and~~ When Bratton's people got ahold of this they got real excited about it, and Bratton came up to see Hurt and he told the rest of us that it was this was something new, a new window into intelligence had been generated by this message because he suspected from the words in this message that the Japanese and the Germans and the Italians were developin

TOP SECRET

[redacted]

a sort of secret ~~consul~~ codicil to the Tripartite arrangement and he wanted to know more about it. Well as a result of his very honest pressures on us to learn more about it we looked at all the other traffic and we found a strain of traffic that we had not yet been able to decode. ~~and~~ We knew very little about it, and it was pretty much of a mystery to us. We'd made some studies but our efforts had not been strong enough really to get a handle on what kind of a system it was. Well Bratton's encouragement to get more about this particular strain of traffic caused us to make our first mature, from the standpoint of our development as cryptanalysts, mature break into a sophisticated code system. This information was contained in a system that we identified by its solution as a Japanese cipher machine and it is known as the Red Machine. ~~and~~ This was the first time I think well I'm sure so far as the Americans were concerned, it was the first time a foreign government cipher machine had been broken. ~~and~~ The results were sort of overwhelming because we mechanized the well first in our solution of this machine, we availed ourselves ~~to~~ of the IBM equipment that we had rented. ~~and~~ This certainly enabled us to do much more cryptanalytic work, much more sophisticated cryptanalytic work ~~and~~ in much less real time than had ever been visualized even in our wildest dreams about the advantages of

[redacted]

code of the automatic accounting machine installation. Now we were so successful is one way of putting it or the Japs were so stupid in their choice of a cryptographic system that we were able to sort of later on lay out a full ~~vest~~ vista of this machine for several months in advance of its use so all we had to do was to ~~tie~~ the keys as the messages came in and decode them, ~~and~~ since we built some pretty primitive automatic machines to do this, we were able to provide G-2 with first class intelligence while we went on with our researches, and this is important from the management standpoint. Researches into other areas of intelligence production and into better equipment for use by the US forces and into a greater potential for cryptology as we look at it on a broad base across the government. And if you don't generate this forward look, if you don't solve the systems of tomorrow by your work on what you've got in front of you today you are then perforce going to get behind the operation, and this is always the fear that the administrator must have when he looks at his operation. I am investing the right amount in the forward look to solve the systems of tomorrow and to improve our cryptography of tomorrow whether or not I'm getting anything out of it today. Probably one of the questions that needs to be answered in connection with our early activities, I have mentioned the use of the Second Signal Service

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

which was run by the Chief Signal Officer as his operational activity aimed at satisfying parts of the intelligence requirements which were imposed by G2. Now how sort of did this develop and what kind of administrative arrangement was early employed in the integration of both the cryptanalytic unit, which was Friedman's technical group, the collection of the material on which this group worked which was the Second Signal Services role and, as we look at it from our sophisticated viewpoint of 1975, what sort of requirements were generated and who produced these requirements? Well to deal first with the obvious, certainly there was no point in the Chief Signal Officer trying to produce intelligence which wasn't required by G-2. So G-2 laid out the broad terms of the requirements, and I touched on that when I indicated Japan was the highest priority. Well now looking at it in the practical world of what limited facilities we had for collection, and they were real limited as you compare it with what I can imagine are in existance today, something like 100-150 trained intercept operators in 1936 and these figures do bear checking, but there were lots of people called intercept operators but we had only a few good ones, and of course Japan being on top it was barely enough to make a dent in '34, '35 into the requirement for Japanese. Now requirements don't seem to be important if you've got one

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

requirement which will absorb more than ~~the~~ your resources. There's no head-scratching or decision or argument about it. You do the obvious, ~~and~~ so in those days there was really no squabble about what was to be done. ~~G2~~ G-2 didn't know enough about it, the users' intelligence didn't know enough about the problem to say cover this link or cover that link, that got invented only when Bart Pulling and some other people tried to do some ~~[illegible]~~ incubation here which was completely uncalled for when AFSA was formed, so the idea was to intercept the message, try to get those that contained the best intelligence and the people who knew about that were the fellows who were breaking the codes, ~~and~~ since they translated then the broad requirements of ~~G2~~ G-2 into the narrow requirements of what links to cover they sort of had the key position, and I think that is right because they're the ones who can look in both directions and the other two look from the ends of the line.

Since it's rather difficult to do what I'm trying to do here today, namely try to talk about the administrative angles of the cryptologic process without my calling to mind some of the actual, practical, historical developments, I'm going to talk a little bit about the history of our undertaking the broad based operation against

TOP SECRET

other nations other than Japan. In other words we're broadening the response of the cryptanalytic and intercept organization to the broader priorities of the G-2 requirements. We're going from the simple requirement of the Japanese into German and Italian and others. In the years between 1934 to 1939 which roughly bracket the (time when the) intelligence effort against nations other than Japan was undertaken, we finally completed our code compilation requirements and were able to spend more time looking at better ways of solving systems and what to us was very important at that time, the development of more skills in our staff. We had been able to get enough funds to hire additional cryptanalysts and one of the greatest things that happened I think was bringing Leo Rosen who was an electrical -- electronics engineer, graduate of MIT and a very brilliant man to sort of bring to bear on the cryptanalytic process electronics engineering. Friedman had some skills in this, I had some but outside of these which were rather accidental most of our skills were mathematical and linguistic in those days and we really had no proper research and development activity. Now while it was assumed and somewhat appreciated that science and engineering would play a great role in the future of cryptology, actually in those days there was very little opportunity to test this concept and Rosen's arrival I think was the first real

TOP SECRET

TOP SECRET

break into the use of modern, as we looked at it in those years, modern technology and its direct introduction into the cryptologic process. A couple of things happened that I think throw some light on the adminstrative problems ~~that~~ which had to be solved. The Japanese introduced the new machine to replace the Red which later was known as the Purple and this was an entirely new principle and those of us who were involved in Japanese problem got kind of shook up because this real pat solution we'd developed for the Red machine went out the window while they were still using it. The bulk of their current important traffic, That is the Japanese Foreign Office important traffic, was sent in the new machine which we hadn't solved. We had a year and a half's interlude of breaking into the new machine which in effect was the reinvention of the Japanese machine ~~and~~ From an administrative standpoint I think its important to note that these years of non-productive -- non-productivity of probably the cream of the cryptanalytic staff had to be tolerated to recover from a simple change of the Japanese cryptographic administrators to put in a new code machine, ~~and~~ This simple decision on the part of the opposition created a rather extensive series of decisions on the part of the office of the Chief Signal Officer in G-2 as to how they would cope with the situation

TOP SECRET

TOP SECRET

which resulted from the simple decision of the Japanese. So adjusting to this made us realize there were certain other problems which had to be dealt with. Namely these were how to dispose your forces so you could satisfy your requirements of the code production program which we had in front of us, the production of intelligence from other fields and then the recovery of this small source of intelligence which by now G-2 had developed a real extra-ordinary appetite for, and They wanted some of the old food which they had been raised to be served up in front of them, and the tolerance of both G-2 and the Chief Signal Officer of allowing us to take the cream of our crypt-analytic talent gambling that we would be successful in reading this new Japanese Purple Machine and I think it taught us a real good lesson. Namely this was a worth while gamble and it was a good practice to follow. Now as an outgrowth of this we of course had certain side benefits which accrued to us. We had a better understanding of the weaknesses of the machine. What were bad practices in applying machines because by now the Signal Corps had introduced the old M134 into practical use and we were having all sorts of problems trying to find out what kind

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

of procedures were the most secure which ought to be followed in the code room. Our work and experience with the Japanese and our success told us what were bad experiences, so we folded these right back into the improvement of US cryptography. Now I guess this is a good point for me to put in a plug for my own concept of what's important. Most people, in my experience, have sort of assumed that the production of intelligence is the epitomy of the cryptologic effort. I disagree. It's pretty high up but it certainly not the top. The most important goal of the cryptanalyst, the fellow who understands the operation of the codes and ciphers and cryptographers and that's the total process, is to fold this back into the improvement and to produce the ultimate in cryptography for this government. All these other things are incidental to that one particular point. And I think we learned at that time that the best way to learn what is good in cryptography is to discover the weaknesses and to capitalize on the weaknesses of the use by foreign governments of their own cryptography. Probably the greatest thing that came out of these early years, the 1930s, developed after we had successfully solved the Purple machine the Japs had introduced, and the work we did at that time was to solve a Japanese transposed code system, which was a very sophisticated type of thing and I don't

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

think I'm doing Billy Friedman ~~doing~~ a disservice saying that he actually did not think we would be able to recover this system cryptanalytically. But he didn't discourage us. He was simply telling us don't be disappointed if you don't because he had faith in our ability to do whatever was needed to produce intelligence from this. Well the important thing about this system from the perspective we're looking today is that we opened up a door into the total vista of the application of computers to cryptanalysis Earlier I've mentioned that we had built ourselves the standard IBM equipment which in itself is a great step forward but looking at it in the context of what I'm going to say right now, that was the first step necessary to first step to the second step which I'm going to describe to you. In our work on this transposed code system we found out that the so-called hand methods or the standard equipment accounting equipment methods that we had developed just were not adequate to deal with the cryptanalytic task which we had in front of us so we rather in a rather primitive way modified the existing equipment to produce a new breed of equipment which I reckon turns out to be the first practical computer that was ever built probably in the world because most of the other effort had been just directed at showing that you can do these pencil and paper things mechanically, and here we had another problem to

~~TALKS VIA COMINT CHANNELS ONLY~~
~~TOP SECRET~~

solve mainly do them mechanically and with a greater profit so we devised a scheme whereby we could modify these standard equipments and actually developed a rather primitive computer which did an amazing thing. It enabled us to actually stay current with the requirements of solving I believe there were four keys every day that had to be recovered. Each one was required a great number of man hours if you did it by the old tried and tested pencil and paper methods and we just didn't have enough staff nor could we ever hope to get enough staff to achieve this solution. But the challenge here was just enough ahead of us so that we could achieve a practical solution by modifying what we had in front of us. Although it took about ten years and a war in between to show that computers could be used to tremendous advantage in the technical requirements of intelligence production and the improvement of our own systems, we did set the groundwork, and actually we had to develop another thing which from an administrative standpoint is awfully important. A sufficient understanding of the scientific and engineering processes to adapt these to the cryptanalytic process before we could really get full benefit from them. These feeble efforts early on which arose from our Japanese problem simply told us and proved to us that we had to develop this capability before we could really realize the full

~~SECRET~~

benefits of the upsurge in the computer technology which we're all familiar with as having happened as a result of WWII. Historically we're now just about three years ahead of WWII, ~~and~~ It was beginning to be pretty clear to the planner and policy makers of the US government that war was coming up. Certainly we had to be ready for it whether it came up or not. The world situation was right nervous, and in the next two or three years I think this nervousness became much more apparent and finally we did get in the war. But because of the tripartite arrangement and because of our ability to read without any delay whatsoever the messages from the Japanese foreign office to its ambassadors in the key capitals of the world we had a pretty good feeling for what was going on in the Japanese mind. We also had a pretty good feeling of what was happening in the German field because Kully and his German effort, he was heading up the German effort at that time, had broken in to one of the more important German diplomati codes so that there was some reaction, certainly not as full as we had from our total reading of the Japanese because the German one-time pad had not been read at that time feeling that things were getting more and more nervous Finally Mr. Roosevelt sort of let it be known that if we were going to get into this struggle we certainly would

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

TOP SECRET

side with the British, then of course the war broke out in Europe why things crystallized and we were sort of galvanized the whole government was galvanized into action and one of the things that happened was the augmentation of our cryptanalytic staff because this was given extremely high priority by both ~~G2~~ G-2, the Secretary of War at this time was vitally interested in this thing and the President too because the President was privy to he actually read the decodes the translations of the decodes of the Japanese messages with great interest. Well first thing we did was to call in all the reservists of the ~~G2~~ G-2 and the Signal Corps who would be used, brought in ~~Roleson.~~ Rosen -- He was a reserve officer. We found this was a good thing so we searched through the ROTC files and brought in a lot of people. Dale Marston is the one I think of as probably the most significant of the type of people we brought in and he's only one. There are any number who came in in that second wave. Then when war actually broke out we were confronted with assembling a whole bunch of linguists as well as mathematicians and training them and we were confronted with other problems like where are you going to house all these people that you've collected, and how are you going to get the right amount of equipment and other things which they need. Even pencils and paper become

TOP SECRET

problems that would have to be solved. These problems -- there was no war plan in cryptology that made any sense because you didn't really know from one day to the next what your requirements were going to be. But luckily we had people who had guts enough to make a good decision. We built two buildings instead of one at Arlington Hall Station to house the Army and the Navy took over a girls' school just like the Army took over a girls' school and they had plenty of housing and first thing you know we had plenty of room and plenty of people and

Tape 8, Side 2

how I don't really know to tell you about the solution of these administrative problems except that we had clever people who had guts enough to make decisions and that those of us who were on the using end took the time and spent the effort to make the best use of what was made available to us. In other words we had to take a chaotic situation and make some kind of reasonable effort out of it. Now you cope with the problems as they come in in a case like that. The broad general plan was to get more people, more facilities and more resources and you've got almost unlimited money in case of a war to draw on, and you've got almost unlimited manpower to draw on in the

[redacted]

case of WWII. So we just did the best we could. It was wasteful. We had to ~~make~~ correct a lot of mistakes but some of the mistakes turned out to be wonderful things. For example Frank Bullock's decision to build two buildings down at Arlington Hall Station was one of the wisest decisions he ever made, yet he was criticized when he asked for the second building that you'll never use this and his answer was, "Well if we don't use it for this we'll need it for something else. Let's build it." And we needed it. Now I guess the administrative lesson from what I've just said is that in emergency situations the rules and the rule book just don't apply. You do the best you can with what you've got and you use your head the best way you know how. And I think I've described the chaos which we had to clean up in the few months after Pearl Harbor. Now there was another, once we got the people on board, once we got the training program set up, and once we got the space to work in, and once we got the IBM and other gear needed to carry on this activity, and once we got the contracts rolling for the new cipher machines and other things, the administration became pretty straightforward. But the next critical time was when we decided to pull back the effort and you can just imagine the five-wheel, heavy five-wheel going at high speed and how you put the brakes on. How you stop that

[redacted]

[redacted]

Cadillac that going 95 miles an hour and stop it in a hurry because at the end of the war everybody was anxious to go back home. We and the British were sort of pacing each other and how to get back to normal operations, how to demobilize really and here again chaos came in and we had to make the best solutions we could. Unfortunately the rules got changed about every two or three days so we finally did the best with what we had and looked in other directions and just took the blame if something went wrong and if it was right why then we used it to qualify our future decisions by saying well we guessed right before why couldn't we be guessing right now? And from an administrative standpoint there is no way of planning this. You just deal and you cope.

Q: ~~One of the problems which~~

A: One of the problems which began to emerge just before -- well about 1940 was how to divide the cryptanalytic pie or the intelligence pie. This didn't apply to cryptography just the intelligence pie between the Army and Navy cryptanalysts. Developed well a little before the war started. Once we got actively involved in hostilities there was so much more to be done than we had facilities to apply that the problem never bothered us. But now when the end of the war came and the problems of demobilization

TOP SECRET

of the tremendous workforce that had been accumulated by both the Army and Navy for the war time effort and what to do for the post war effort as these problems began to emerge, then the problem of collaboration between the Army and Navy became the worst administrative problem that had to be solved. And this surfaced for very good reasons because both of them, both the Army and the Navy, were asking for funds you see for enough of an effort to satisfy the US government, and One man in particular, Kenneth ~~Royall~~ Royall, this was just about the time the Department of Defense was established, Air Force came up as a third service, and when the Air Force put in for a similar organization which would be at least as grand as either the Army or the Navy had, ~~Royale~~ Royall threw up his hands in disgust and went up to see Forestal and ~~said~~ says, "We cannot have this, this is going to break the back. ~~It's~~ He says going to wind up with something less than a good effort. Each of the services are asking for funds to do exactly the same thing and we just can't tolerate this." And Forestal who was pretty much of a problem avoider instead of a problem solver simply tried to duck the issue. But so much steam was generated by ~~Royale~~ Royall that finally a board was set up to determine just what sort of effort would take place and it was this study of the --

Q: Was this the Stone Board?

TOP SECRET

A: Yes. It was this study that generated the proposition that a central organization, a defense department establishment would be developed for the cryptologic activities of the US government. The board was known as the Stone Board headed by Admiral E. E. Stone. After several months of deliberation, most of which was acromonious, the decision was taken back to Forestal's desk by Secretary Johnson, Louis Johnson, to set up one organization known as the Armed Forces Security Agency, and this he got Mr. Truman to initial and came back and laid on the backs of the Army and Navy and Air Force. and I want to tell you gentlemen if there ever was an administrative problem of extraordinary dimensions it was how to consolidate the old ingrained Army and Navy organization and this brand new sort of still wet-behind-the-ears Air Force organization that the Air Force had been rapidly developing trying to beat the gun on the consolidation move, and I speak about this honestly because openly because it was the way it was. Politics of the services were rampant. The administrative decisions were not decisions based on necessity. They were decisions based on political prestige and power and this was an extremely difficult set of decisions to cope with. Finally when the President initialled this

[redacted]

there was no question ~~of~~ but what it had to be put into ~~effort and~~ effect. Then the type of decisions which had to be made were those which had to somehow marry the prestige of each of the services with the actual requirements of the problems. ~~and~~ Even though this was a difficult thing to do, it was still ~~simple~~ simpler or at least in my view to solve these problems then it was the problems of collaboration and the switching of problems between the Army, Navy and the Air Force because there were ~~other~~ a lot of artificial and not very well understood rules that were being applied to the collaboration between the services before the consolidation took place. I don't think I ought to say any more other than to note there were terrific, probably the most chaotic administrative situation in the history of cryptology that took place at about the time that AFSA, later NSA, was formed. But this was the real administrative mess. I hope by today that some of these old service philosophies and political and prestige aspects have been forgotten and that we can all aim ourself at getting on with the problem, but I rather suspect that they still are here and that maybe you know more about them than I do.

Tape 9, Side 1

In early '30s after we had reasonably completed the training program Friedman had laid out for us and started work on the code compilation program, the big codes that were really to become the stopgap between the cryptography of 1930 and the advent of cipher machines which really didn't take place until about the time, shortly after Pearl Harbor when, ABA (SIGA) which the Navy called the ECM was placed in the service by both the Army and Navy. A lot of things took place that probably ought to be explained. One of the most important features of this era was that those of us that had been selected for training Abe Sinkov, Solomon Kullback and myself, later on supplemented by Bob Furner Albert Small, and Leo Rosen, and, in turn, supported by some very able officers such as George Fisher ~~Beecher~~ and Harold Hayes, Col Harold G. Hayes, Corderman to some degree. We had begun to develop a pretty solid cadre of people who were knowledgeable in cryptanalysis. Now the level to which cryptanalysis had been raised by Friedman in his work up to 1930 when we joined him formed the foundation on which the future advances in the field of cryptanalysis and ~~the~~ indeed in cryptology because the cryptanalytic advances were folded back into cryptography and the whole field of cryptology was consequently promoted. This arose probably because Friedman's understanding of cryptanalysis was based fundamentally on the statistical and analytic approach rather than the procedural approach that were followed by most people

~~TOP SECRET~~ ~~COMINT CHANNELS ONLY~~

~~TOP SECRET~~

TOP SECRET

who came into cryptanalysis through language. Friedman had a feel for the mathematical process although I don't think he would have ever admitted that he was a mathematician. But he certainly had a feel for the application of mathematics and an understanding of how mathematics could be used to advantage. ~~and~~ He was in love with the analytical approach even to the degree that sometimes he at least in my opinion carried his analysis much further than was merited by the nature of the problem. In some cases he would, for example, ~~he would~~ prefer to use the analytical approach over what we called the "golden guess" or the probable ~~proper~~ word approach. ~~and~~ If he had any faults it was because he too firmly believed in the analytical process and sort of psychologically avoided the shortcut or maybe he thought it was really cheating to get the answer without doing it the hard way. Now with this kind of a background in psychology we all Kullback, Sinkov, myself and the others I mentioned had a better appreciation I think of the importance of analysis and a greater dedication to it than had ever been encountered in any group of cryptanalysts before, and because we had been so carefully selected with certain mathematical training and instruction it was easy to build on this so that what little powers we had when we first came in were augmented considerably by the training and experience which we developed. Now we as part of our preparation for in the training preparation Friedman

TOP SECRET

had us study all the machines that he had collected. There were such things -- well we started off with the simple ones like the ~~Wheat Stone~~ Wheatstone device. Then we studied the Kryha which was not much of a cipher machine as far as security was concerned but which certainly was a practical exemplification of mechanical encipherment process, ~~and~~ we also studied the B211 which became a little more sophisticated as you look at it in the scale of complexity. Friedman's work, of course, on the ~~Hebron~~ Heburn machine, -- He helped us through that. We didn't duplicate it but we certainly understood it completely before he got through with ~~it.~~ us. The challenge that we accepted on the Mark II ~~Hebron~~ Heburn which had been put together by the ~~Hebron~~ Heburn concern for the Navy and we successfully met that challenge and with the result the Navy felt a little bit -- well the Navy had to go look for another device because we proved that the Mark II ~~Hebron~~ Heburn was not satisfactory for wide spread Navy usage and wouldn't stand up with the terrific strain of ~~the~~ normal naval communications, although it was quite adequate for special use, or small volume situations such as for example sending in enciphered intercept traffic from an intercept station that had to be transmitted by radio, you could use the some of the old Mark II types for enciphering this very limited, very specialized strand of traffic, ~~and~~ the only reason you could do it is because the volume of usage ~~is~~ was such that it didn't overload the circuits and consequently cause the machine to be compromisable by

~~DIPLOMATIC CHANNELS ONLY~~

~~SECRET~~

cryptanalysis. [Another one we worked on which ought to be mentioned
DoS is the machine developed by Col Parker ~~Hit~~ Hitt for IT&T which was
presented to the State Department as possible use.] We were
real lucky on that because we'd just gone through Friedman's
exercise on the recovery of the ~~Vernun~~ Vernam machine and since this
IT&T development was another modification of the application of
a keystream generator electrically to the message stream
information by a simple relay additive box that was hooked on--
attached to the teleprinter, why we had very little difficulty
in mastering the IT&T device. Now the IT&T device differed
a little bit from the ~~Vernum~~ Vernam, Well essentially different from
the ~~Vernum~~ Vernam in that it used a bunch of cog wheels, gear wheels
with moveable pins to generate the keystreams, ~~and~~ It was not
too well designed by Hit, and we had a lot of luck and a lot of
fun in breaking this in record time because we did a couple of
"golden guesses" and got the answer. The first of the challenge
messages in a remarkably short time. I think you should note
that ~~Hit~~ Hitt, although he was greatly disappointed that his invention--
his design of the cipher machine fell short of much short of
DoS the security requirements [of the State Department], was quite
pleased that the War Department and the Signal Corps had developed
a capability for dealing with something which he as an old-time
cryptanalyst thought was first class cryptography, and deal with
it in sort of a mockery of his work. Instead of being sore he
congratulated us and I think really sincerely pleased that we'd
been able to break ~~[illegible]~~

TOP SECRET

his machine. Other machines we studied were the Hagelin, the earlier models of the M209. There were two or three of these, I think they were in C40 - C30, well I don't remember the exact nomenclature but basic Hagelins; thats with the five or six wheels, the pin settings on the wheels serving to generate the key which then was used to control the movement of the, well they use direct and reverse normal alphabets on the print wheel. Of course the big difficulty with this machine is that ~~the~~ two messages using exactly the same key that is two messages in depth could be read without too much difficulty, and if you got enough of these you could recover the pin settings and reproduce the entire machine. Another thing we studied was you have a intensive, a rather exhaustive study of the strip cipher ~~system~~. The reason that came about is because it is necessary to develop a cipher machine for joint communications Army/Navy units. ~~and~~ There were no mechanical devices available, and the prospects of printing up special codes for these purposes was both time consuming and expensive, (it was) so more or less agreed to use the strip system. The only cryptograph, you couldn't, shouldn't call it a cipher machine that was available at that time for official use within the either the Army or the Navy any where in the US government was the old cipher device M94 which was had been earlier produced by Hit and ~~Mobern, Col Hit~~ Mauborgne, Colonel Hitt and General, well later General ~~Mobern~~ Mauborgne, who at one time was the Chief Signal Officer particularly in the days when we were having much more spectacular successes that we

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

TOP SECRET

really thought we would have. Interestingly enough the work we did on the strip cipher device was quite inadequate for a thorough test of its security. The test was based on a set of messages. I think there were something like over 600 lines of cipher text - 25 letters in length that had been enciphered by a simulated strip cipher device which we were given as a test problem, ~~and~~ Abe Sinkov and Solomon Kullback and Frank Rowlett studied this very carefully and all ~~he~~ we succeeded in doing was to prove that it was impossible to solve, This number of lines of text enciphered with the strip cipher device. We did this because we pursued the analytica approach too assiduously and we went away sort of feeling reassured this was pretty good device and Friedman went away reassured that it was a good device and told the Navy about it, and everybody agreed then to adopt the strip cipher system ~~that~~ as the basic system for joint communications between Army and Navy. Later on a couple of the students, I believe was Capt Brown and his team had the same problem. I think Friedman gave it to ~~him~~ them because he wanted to now these were two military officers who'd come in and joined in the cryptanalytic training because part of the concept was to train officers as well as civilians in cryptanalysis so that there would be at least a few people in the military establishment who had an understanding of the crypto-graphic process and cryptology and some understanding of cryptanalysis. Well these two fellows instead of approaching

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

it from a mathematical, analytical approach found numerous repetitions at the beginning of these messages and started guessing such things as battalion and enemies advancing and whatever beginnings they thought might be plausible from the form of the text, and of course they could check them out because the letter could never encipher itself in the strip system, and In about two weeks they had had enough proper words that they were able to reconstruct and develop other assumptions in other lines of the text, and within well a startling short time after that they had recovered a set of strips, and We all learned a very good lesson from this because instead of just flashing your cryptographic system against one technical approach we learned that you better flash it against everyone because the analytical approach, while it might be the only thing that will produce results under some circumstances, Under other circumstances does not permit the solution to be obtained, and If you take a few short cuts and combine analysis for example with the probable word system approach then the system itself may not be so impregnable.

Now another sort of important thing which developed in these years was that some of us got the opportunity to work in the code room, War Department code room and actually observed what processes needed to be followed in the handling of traffic, and We found out by our contacts with the coderoom personnel and watching the code clerks who were at that time being trained

to handle the War Department codes and also in our work in training operators for the M134T1 which came a little later on, we found that it would just be impossible to expect code room personnel who were given only very limited and very specialized training to do much more than sort of routinely apply the rules which they had been exposed to in their training program, and that if anything we could expect them to be human and to make a lot of mistakes, and the systems therefore had to be designed so that they would resist the mistakes made by the code clerks because we found in our work on the cipher machines that I mentioned earlier and through watching what was happening and particularly through the probable word approach that these two officers used on the strip system that a lot of opportunities for exploitation even what would seem to be a very good theoretically secure system sometimes just couldn't be achieved when it was put into practical operation. As time went on we became more and more sophisticated, and our experience was expanded through the work on the Japanese codes and we learned quite a bit from that. We were able to marry the information that we had developed, our power, our cryptanalytic power if you will which we had developed on our training program and our work on Japanese with the requirements for the development of the secure and automated type of cryptography like the cipher machine that was required for code room operations at high level or for field

operations in terms of the field cipher, to marry them so we could begin to visualize the kind of apparatus which would be needed for securing US communications in wartime. There had been I might point out that there had been lots of impulses in this direction. This had long been Friedman's objective. If you have an opportunity to go through Yardley's papers you'll find that he had advocated machine cryptography, and the Navy in their efforts at having Hebron trying to develop a cipher machine was also dedicated to this. Hit and Mobern had long had dreams of automatic cipher machines and we were now beginning to appreciate the importance of teletype systems instead of hand telegram systems for very mobile situations, battle situations if you will because the Army was installing teletype machines to be used in support of the manuevers which they were conducting and some of us got an opportunity to actually go out in the field I know I was sent to San Antonio, Texas just to watch the manuevers and stay around the communications centers to see what the field situations were like. And this was particularly important because we'd planned to use teletype for the first time in a field situation and it had a tremendous impact on me as an individual who had been trained in the war department code rooms procedures where we were using these awkward old code books and we typed up the encoded message on a radio blank and hand it to the radio operator. To see a teletype operator would just take a little old message blank

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

that somebody had written a message on in longhand and stick it in his teleprinter and send it several miles to the next installation, and it was quite easy for me to visualize some kind of a black box hooked onto this teletype and the one on the other end operating like the ~~Vernum~~ Vernam device was supposed to operate to provide high degree of security for field communication in the ~~A~~army, so all these things taken together developed in us a real appreciation, I'd say a pretty sophisticated, in those days, appreciation of what might be done with the improvement of US security and we fully realized, I think its important to note, that you could obtain the ultimate US security only if you had a full appreciation for the cryptanalytic weaknesses of the principles that were to be employed in these devices that were to be hooked on, for example, the teletype system or be incorporated in the machines used in the War Department code room.

At about this point without reference to the year in our development of cryptanalytic appreciation or power if you will, something happened which I think was pretty important. The first models of the first cipher machine that had been was going to be practically used by the war department were coming off the assembly line and were to be put into effect in the War Department code room and in the headquarters of the three overseas departments and I believe also at San Francisco in the ninth corps area. This was the M134T1. It was a five-rotor device. The movement of the rotors were controlled by a punched tape which passed through

~~UNLESS VIA COMINT CHANNELS ONLY~~
~~SECRET~~

a head and each hole as it appeared in the tape and each one of the streams would tell a cipher wheel of the set of five to move forward. If there was no hole of course the cipher wheel did not move and the motion of the wheels then was controlled directly by the perforations in the tape and each time that you depress the key the tape moved forward one and so it was basically a real good principle. Theoretically sound and you could never use the same tape twice, obviously it had all the advantages of one-time tape or one-time code system. This was the greatest thing that had happened in cryptography up to that point in time so far as the US Army was concerned and well in advance in sophistication of any other device that we'd studied or heard about. I didn't mention that we studied the Enigma. We didn't really study it, we examined it. The others that I mentioned we had studied in our training program but we never did set up a problem where we actually solved an Enigma machine and recovered the wheels, the wheel wirings of an Enigma machine but we developed certain theoretical studies which we thought would be effective if the machine was used in volume. We just never had time to make a thorough and exhaustive study of the Enigma device. But we felt from our understanding of the machines we looked at successfully studied two solutions that we could sort of extrapolate from our knowledge of these and work out the solution to the Enigma and probably one of the reasons we never went after the Enigma with more fire in our eyes is because we had no idea of how the indicator system that would be

TOP SECRET

used under practical application of the Enigma would work because usually at least in our thing at that time big trouble was solving of the indicator system rather than the recovery of the machine. If the indicator system was poor the solution of the system might be a snap. If it was real sophisticated indicator system of course it might offer more problem in solution than the recovery of the machine. Now the M-134, using the tape for keying the advancement of the wheels, was far in advance of the Enigma and at least in our appreciation of it at that time and the indicator system was not at all vulnerable because it was simple enough to apply and yet powerful enough when it was applied to make it extremely, well we didn't know how to solve it at that time. I think with today's technology it might not offer such a problem because we now know better about the terms of use of these things, but at that time it looked pretty doggone good. In due course the machines were received and sent out, installed. Friedman was able to take the machines to Panama and to the other two overseas departments and install them and observe the coderoom operations involved in enciphering and deciphering messages and he stayed there and worked with -- actually worked with and in the coderoom getting the machines insuring that the machines would work and insuring that the coderoom operators knew what they were doing and wouldn't make too many stupid booboos, at least while he was there. The big problem with these machines as I recall was, at least the one that I was involved with the most was the generation of the key tape

TOP SECRET

because the state-of-the-art in keypunching had not advanced too far. It was fine to use a very fine piece of papertape such as Western Union used for typing up the message, and if you're going to use it only once or twice through that tape head and if it was plaintext and you tore a hole in that tape it didn't make too much difference. But when you were using a piece of tape to control the movement of the cipher wheel, and if one of those holes was mutilated you got an advance or the wheel didn't advance and from then on the message was indecipherable. So it was very important to have key tapes which were accurately prepared and which would endure use and reuse and reuse for several days -- maybe several messages and ~~under the~~ more of the tapes which we could buy at that time ~~set~~ stood up under this multiple use requirement. So we began soon to recognize that there were a lot of problems, coderoom problems that is, as well as production problems in using the key tape as a keying element on the M134. I think our biggest problem at that time was not the lack of ideas for good cryptography ~~as~~ with its principles which could be incorporated into devices, but probably the state of the art of ~~the~~ manufacture of cipher machines because very little experience had been achieved in this field. The few rotors which had been built for the Hebern machine and the M134T4 were, I would judge by todays standards, more or less experimental and the materials used, well for example, in the rotors of one of the devices, the material was abrasive and we would get shorts between the

SECRET

related contacts, adjacent contacts, and the cipher wheel because metal particles had been embedded in the bakelite composition material that had been used for the construction of the wheels. ~~and~~ This is only one of many other things. Since the M134T1 used solenoid-actuated mechanisms for advancing the wheels, These still were more or less in the experimental stage. They weren't really tested by operations. There were many failures of these particularly in the M134. ~~The~~ Then one defect that I remember vividly is that they were very fragile devices, ~~and~~ I can recall watching Major Reeder supervising the unloading of the shipment of these devices from an army truck, ~~and~~ the enlisted man who was unloading the device when Reeder told him to unload that one first picked it up by the end and end over end it out, and it fell about four feet from the body of the truck down to the concrete platform on which the truck was parked, ~~and~~ I can see Reeder holding his hands to the side of his head in agony ~~and~~ until when they took this thing apart, ~~and~~ the guts were all in one mess when we opened up the case in which the cipher machine was enclosed that it destroyed the machine. In the long run this was a real break because it gave us a keyboard and a solenoid operated typewriter to experiment with which we'd never had if we'd had to cannibalize an M134. Machines had to be rugged, obviously because in this experience of watching the enlisted man unload the first machine from that truck, if we needed any proof

HANDLE VIA COMINT CHANNELS ONLY

SECRET

SECRET

there it was, so we had to set up a whole new set of parameters based on the little experience we'd had with the 134 which would have to be brought in to play at the time we produced that machine which would be the answer to all our machine requirements. Now I've sort of digressed and gone into the problems of cipher machines developments here, but this and the advances in our understanding of the COMSEC requirements because now they were much clearer to us than they'd ever been to any set of people before based on our experience through the analysis of the machines I've mentioned and the practical experience with the 134 that Friedman had received through his installation and that we observed in our testing of the machine both for operational and cryptanalytic security. In the other domain that is the broader requirements of the production of intelligence we had reached the point of where we felt that there wasn't a Japanese diplomatic system that we couldn't read given a reasonable amount of intercept and a couple of months time. ~~We were~~ At that time we had read the Red machine and we were well into the Purple, ~~and~~ There were other pressures being brought on us both in the intelligence field and in the COMSEC field, and these pressures were to produce intelligence not just on Japanese but on German, and Italian and certain other countries, France as well, Spain, some of the South American nations, and to produce at least have drawing board designs of field ciphers,

TRIBLE VIA COMINT CHANNELS ONLY

TOP SECRET

mechanical devices for use by army and division message centers at army and division level message centers in the Army and these would be needed in quantity of course if hostilities broke out. ~~and~~ So our requirements were beginning to be multiplied and the pressures were building up because the war clouds were beginning to become more pronounced as we looked at the world situation in those days. We're now getting up around 1938. Also it became evident that while we were being held back by the state of the art developments in mechanical sort of model making and electrical electromechanical manufacturing techniques and materials, we were short of people skilled and trained people and plans were being made and courses were being introduced into schools and universities to use ROTC students and the training of the reserves Signal Corps reservists in cryptography. ~~and in particular~~ We hadn't reached the point where we wanted to train the reservists in cryptanalysis but a lot of training courses in cryptography were being produced for the ROTC and the reservists. ~~and~~ There were two special texts ~~techs~~ number 165, Elementary Military Cryptography, and 166, Advanced Military Cryptography were being taken by great numbers of reservists and by ROTC students. ~~and~~ Special courses were being conducted ~~and so~~ in a couple of the schools for these ROTC classes. Also we got additional funds for hiring more people. ~~and~~ In those days we spent a lot of time of the new recruits in

[redacted]

training. We made sure that everyone was exposed to some training in all the cryptanalytic techniques that we had developed, and, while it was impossible to train them in the more sophisticated techniques of machine analysis, we did train them in the procedural steps which were required in the application of the more sophisticated machine analytic attacks. So we were beginning to get a pretty well balanced team, some people with long term, broad, comprehensive understanding of cryptanalysis, and some people with somewhat shorter term but very specialized training who could be integrated into special teams for attack on such things as we learned the lesson from our practical experience in breaking the Red Machine, the Purple Machine and our security analysis of some of the U.S. systems that we had undertaken. How to develop the team concept to build a team with a good technical leader supported by lesser technical lights until we could get a very efficient application of manpower resources and produce results in a short time. Another sophistication, I guess that's about as good a word as I can think of, that we developed was in the application of accounting machines to cryptography. We'd been able to procure a small installation of IBM equipment and we thought this was much better for our purposes that the Hollerith which at that time was about equal in its importance of its business applications to IBM. The reason we chose IBM was the flexibility afforded by the IBM plugboard, particularly in the

TALENT KEYHOLE COMINT CHANNELS ONLY

SECRET

TOP SECRET

reproducer and the tabulator applications, because we could wire from column to column and sort of at will in the IBM whereas the Hollerith had a smaller card field and the machine had to be mechanically contrived. and so it was impossible ~~to keep the~~ for the operator or the user of the machine to modify the reading of the card. ~~so IBM~~ So IBM was ideal for us because the plugwire ~~was~~ gave us the ultimate in flexibility -- well, ~~the best flexibility that~~ gave us a better flexibility than the other and we needed that flexibility. We needed much more than the IBM could afford us.

We're now, as I look at it, somewhere around '37, '38. ~~This is in that~~ This is at that time in which we weren't really sure we were going to be in a war, but if any of us bet on it we'd have to bet it would be a real proper war coming up pretty soon. At least that was the attitude taken by the Secretary of War and such people as the Director of Military Intelligence and the Chief Signal Officer who were sort of in the front in the war planning game. Of course the steps taken to augment the technical force through the ROTC and reservists was a proper one. Still it was impossible to train these people to the degree that would make them immediately useful for use in wartime circumstances because they were still they still needed the element of experience. I suppose at that time the pressures got so great that it was inevitable that there would be an expansion not exactly an explosion, but a sort of increase in

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

the rate of growth. So we began to get a lot of people to train. We got the reservists in for tours of duties. We got more of the military in. Unfortunately they amounted to only a small amount because the requirements and needs for regular officers at that time had multiplied because of this concept of the imminence of the war, ~~and~~ So it was a little harder to get military personnel. ~~We~~ Of course we augment of our intercept capabilities by getting ~~our~~ more positions authorized, that is both equipment and operators, and the growth in that domain was a lot faster than in the cryptanalytic domain. We began to recognize the need for more people with language skills, ~~and~~ So we pretty soon had to start on a recruiting program getting people who we thought would become qualified as cryptanalysts and people with linguistic skills, ~~and~~ There was always a dearth of Japanese translators because it was extremely difficult to find people who spoke Japanese that wanted to work for the government. Most of the people who studied Japanese were either military and they were absorbed in the intelligence activities, or missionaries and missionaries were awful hard to persuade to work for the government. We really weren't successful in getting the missionary types into our business until the war broke out, and then they readily came and performed nobly ~~and I~~ on old worked on Japanese in particular. Other skills we found many students, second generation, the skills I'm talking about now are the language

skills, Spanish, Italian ~~and~~ We also conducted some courses in Japanese and other languages for the cryptanalysts who had not had the opportunity to study languages either at home or in their scholastic training. When we began to realize the results of our recruiting program

End of Tape 9 Side 1

Side 2 is blank

Tape 10 Side 1

When we first got the IBM machine it was a wonderful thing from the labor saving standpoint and I think this was one breakthrough which is probably not matched by any other development in that timeframe, but now that was the first of two important steps that were taken. First, was to learn how to use these standard IBM accounting machines and cryptanalytic and cryptographic process. ~~and~~ Then the second step was to learn how to modify so they became more efficient and more powerful in the support of our cryptanalytic endeavors. One of the most important aspects of our use of equipments was -- well, the one I think is most important is the modification because there were certain inhibitions that we had to overcome. One of these was the rules made by IBM when they rented us the equipment that no modifications would be made except by company people, company repairmen, company servicemen and without full consent of IBM. That was pretty terrific inhibition. Then there was another very practical inhibition, was did we have people who were skilled enough and clever enough to make these modifications to a pretty complex, electromechanical device that was just about already beyond the point of engineering efficiency. If you did put any more of a load on it it just got

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

so complex it wouldn't work. Well these inhibitions held us back I think ~~from~~ the second phase of the use of automatic equipment in cryptanalysis. However there came a time ~~k~~when we had no recourse except to go in and modify the accounting machines and this came about as a result of our work on the Japanese systems. I don't remember exactly what title it had. We can look it up in the history but the Japanese had for a long time been transposing as a superencipherment process their basic charts and they had dedicated certain charts to transposed systems so they were never used without the transposition encipherment superencipherment. They reached a point however in the cryptographic sophistication where they felt that the simpler forms of I call it group transposition because thats what we called it in those days where you took a 9-or 15- or 13-letter key and applied it in repetition to the codetext to produce a superencipherment. There came a time in their concept when they dropped this sort of simple form of group transposition and went into a matrix transposition of their message. ~~and~~ They sprung this on us without any warning actually and in effect what they had was a modification of the system used by the Germans in WWI known as the ADFGVX system which used a transposition key ~~a~~ something from about 15 to about 25 in length and was applied to a digraphic system. In the case of the German it was a matrix of first five and then six by six identified by the letters ADFG and V for five

and then they added the X I believe or another letter which produc the 36 ~~sixth~~ element alphabet. Now the systems used by the Japanese followed the pattern of the old German field cipher pretty closely It had a key, transposition key which changed I believe regularly. I recall now once a day, ~~and~~ I recall also that there were four transposition keys a day sometime later on in the life of the system and this was applied to the digraphic charts which were dedicated to the system the Japs compiled and issued ~~This used~~ with the transposition keys, ~~and~~ They had added another gimmick which was pretty sophisticated for them at that time of having what we call ~~having~~ nulls or blank spaces at the top of the diagram so it interrupted the logical sequence of the encoded text as it was presented to the matrix for the second step or superencipherment step. Well ~~it~~ actually it boiled down to matrix with certain number of blank spaces at the top and then the transposition key applied across that, ~~and~~ This was in effect for a reasonable length of time, say a day or fourth of a day. When this came into effect it looked pretty awesome from a cryptanalytic standpoint. We'd never really tried our skills on this kind of a system practically The first work that was ~~xxxx~~done on that type of system of course was done early in the training which Sinkov and Kullback and Hurt and myself had under taken. We'd found considerable amount of ADFGVX traffic left over from WWI, and Friedman had saved this because he had worked on the traffic in Europe with the American Expeditionar

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

Forces and in conjunction with the French and he was well aware of Captain ~~Panvan's~~ Painvin's solution of the ADFGVX which was based on repeated beginnings or endings in the text of the message and Friedman had I believe undertaken personally to develop what he called ~~the~~ a general solution which did not depend on this more or less accidental situation of similar beginnings or endings. He had never been able to finish his researches so he wanted this test to be done at some time and he gave it to us as one of our first research tasks in the training program. We were very fortunate. We did develop a technique for the solution of this and I think we can honestly say that had we been available in WWI there wouldn't have been a day's traffic that wouldn't have been completely read by the techniques we developed. These techniques are written up in one of the technical papers called "Solution of the ADFGVX Cipher System" and it was one of the technical papers we prepared. I don't remember whose name is signed on it, but it was a joint work of a group under Friedman's guidance. ~~Now the~~ Actually to summarize this what we found is that the in the time of Yardley no use of superencipherments the form of transposition had been observed. Sometime between the end of Yardley's work and 1935 the Japs began introducing the simplest form of transposition to their code tables and then they continued to increase this and more in the length of the transposition group rather than the complexity of the system until they finally introduced this modification of ADFGVX type of system

~~TRANSLATION CHANNELS ONLY~~

~~TOP SECRET~~

which was a real breakthrough for them. It took it out of the easy into the almost impossible and certainly hard to achieve type of solution. ~~Well I don't remember whether~~ When the Japanese put the new system into effect of course we weren't able to read any of the messages in it. But one of the good things that happened at that time was the Navy were able the Navy second-story types were able to do a job on the Japanese installation and they brought out photographs of the new system that had been introduced and we had full information about this operation. It turned out indeed to be a columnar transposition. Now for a while, while these keys which had been photographed were in effect, we had no problem of course in producing translations, but the Japs soon changed, introduced the second system, took the old system out of effect -- the first system out of effect after a reasonable time I think it was about three months, ~~and~~ Then they introduced a new system. As I recall they changed both the code and the key and then the crunch was on us unless the Navy did some more photographic work we'd have to go back and get the answers by cryptanalysis. Well we'd done enough study on this to confirm the earlier suspicions that it would succumb to the ADFGVX techniques that we developed very early on in our researches and we soon, when we'd accumulated enough traffic, found that by the application of the old ~~Panvan~~ Painvin approach, namely the similar beginnings and ends, we could develop enough statistics about the code chart to give us an insight into

~~TRIPLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

the relationships of the initials and finals as we did a columnar matching in recovering the transposition key even though we didn't know what the underlying code text might represent. The process of course was first to remove the superencipherment and reduce the intercept to basic code, ~~and~~ then after enough basic code text had been accumulated to recover the code so that the message could be reduced to Japanese plain language. Well, our first steps were directed at removal of the superencipherment and we didn't really concern ourselves with the meaning of the code groups because it was the statistical evidence derived from the composit of the code group that was more useful to us than anything else at that point in time. We ~~did~~ needed nothing else but a good statistica table of initials and finals and digraphic combinations. We finally developed a hand technique patterned after the one that had been written up in the ADFGVX report that we'd prepared earli so that we did achieve, I think, some success but we were overwhelmed with the workload. This was a slow, onerous task and we had not develo the experience and competence so that we could recover these keys as rapidly as we needed to, ~~and~~ We therefore were confronted with the problem of developing a better way of going about this. I think one of the impulses that lead us into the development of th new approach was Albert Small's conviction that the process that we had evolved for hand solution could be mechanized, ~~and~~ Small go bit by this concept and he just stayed with it and would not give up on it. The rest of us and I think the rest of us were Friedma

~~TALENT KEYHOLE COMINT CHANNELS ONLY~~

~~TOP SECRET~~

TOP SECRET

e

Furner, Sammy Snyder, you were in on this Sammy, and myself. We did a lot of discussion about how to mechanize the hand proces we'd developed, but most of it was hot air and very little of it was substance because we just hadn't really faced up to the problem and didn't understand the problem well enough at least I didn't to make any sense out of it. Well finally from this, following Small's sort of first impulses about this, we did distill out a technique for a machine processing of the data to satisfy the requirements of this hand technique we'd developed. The only problem was that the IBM machines which we had available had a missing link in it and therefore while we could use them for most of this we couldn't put the program the process into practical application until some modification of the IBM machine had been made. We quite well realized at that time that I mean it was clear to us, really clear to us that unless we did mechanize - although the machines weren't ideally suited for this process - we did recognize we were going to have to use them to some degree and then make up for their deficiencies by hand methods. So from this, Small I believe again was the leader, generated a concept whereby the digraphs of the code were punched onto cards - IBM cards and there were two decks of cards set up, one for the initial final arrangements, and one for the final initial arrangements. In other words it was the statistics based on the diagraph chart frequencies of the diagraphs themselves, and these frequencie of course could be recorded effectively in the chart, and what we

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

did was to convert this chart into the form of cards. ~~and~~ I don't remember just who worked out the details of the wiring which could be accomplished on the tabulator so that this data would be presented in a display so that we could by hand method then sum up the expected frequencies, the statistical frequencies to evaluate whether the specific matches that we were making were good or not, ~~and~~ I might describe what was in this matching process. The concept was to take, make an assumption about how long how many columns were in this transposition key and of course we assume it was the longest possible which was 25 and we'd learned this from photographs. So we took a stretch of text and usually it was the last column the last part of the message and we drug it position by position through every possible alignment of that last column with every other segment of the message. ~~and~~ If it was a 500 position message and we started out with 125th of 500 that was the number of positions less the length of the column that we had to match. Of course we could throw out a few because they just weren't logical in certain places that were impossible on this assumption. But to mechanize this we had to ignore these small positions where it was impossible and just do the whole totalizing ~~turbelizi~~ So if there was a 500 letter message or a 1000 letter message, or a 1500 letter message there was something 500 or 1000 or 1500 matches th had to be made, and all these had to be computed from the display that had been generated by running the cards through the machine.

Now the way we effected this dragging was to use a deck of cards which had been assembled manually from these stacks of cards that Small had prepared carrying the data statistical data from the chart, and what we had was a bunch of bins, 26 bins, and you would take the message in hand and if the message began XYQBW you reach in the X bin and that was the first card, and the second letter was Y you reached in the Y bin and that was the second card of the message, and the third letter you reached in that bin and so when you got through you'd gone to a bin and pulled out a card corresponding to the identity of the letter in the message and that was your message deck. Now this segment, the column that you were dragging against each position of the message was wired into the plugboard of an IBM tabulator so that you read the statistics out of the particular columns applied. What they gave you then was a display sheet. If you wanted to evaluate the expectancy of a match from the sheet you had to take a diagonal, and I believe we start off with about ten values and we used the two-digit logarithmic equivalent to start with, and we summed the diagonal and here I think was one thing that Small contributed to computery that he's never been given credit for. Small proposed very early on many years before we'd worked on this system that instead of using the absolute statistic we use its logarithm because to evaluate the absolute statistic you had to take the product. We had this this was onerous, it was multiplying ten digits, ten two-digit figures together which was a little slow

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

But if you use the logarithm you could add these digits you see and it gave you just you just adjusted your sights a little bit, but it was just as valid and a lot more useful because you could more efficiently produce it. Well we were using logarithms inst of the absolute values for the statistics and our job then was to take a little sort of pattern and lay over the ~~displace~~ display sheet and it lead our eye down the diagonal so we could sum and evaluate th total. Well we finally shortcutted this a little bit as I recoll by taking only values that were obviously above a certain point. If you had a lot of three, fours and 30s and 40s and 50s in this diagonal well, if you had only a few 30s and 40s and 50s and a lot of 10s and 15s and 20s why you ignored it. But if there was a 60 or 70 or something like that then you summed it up because obviously it was an important and high total. Well ~~we~~ I think read a couple of days traffic with this technique but it was just backbreaking and slow and we talked with the Navy about it and th sort of laughed at us for doing this silly kind of a thing and then it was we realized we had to do something a little bit bette Now this diagonal effect here again is where we learned something from the use of from our success on an earlier ~~area~~ machine. This diagon effect was exactly the diagonal effect that resulted from the half Hebern ~~Hebren~~ approach used by the Japs in the Red Machine. ~~and~~ So we conceived of a commutator like the half Hebern ~~Hebren~~ you see which

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

would spread the column reading capabilities of the tabulator down this diagonal instead of having it just a display print the significant figures or the significant figures of the logarithms ~~reading~~ we could feed by the commutator arrangement the data from the chart the data logarithmic value into a counter and discreetly accumulate each diagonal into a counter and we cleared it out after about ten I believe. We could read the totals you see and so it was doing the totalizing for us. Only trouble was that we didn't have that many counters in the machine. ~~and~~ Then Small came up with the idea and I know this was Small - use a single digit logarithm instead of a two-digit logarithm, ~~and~~ then we had enough counters, and lo and behold the statistic was strong enough and all we had to do was to build the daggone device which was hooked on to the IBM tabulator plugboard to do this automatic changing of the wiring.

At this point in the evolution of this process the construction of the device and the design of the device automatically to change the wiring was the point we had to achieve. ~~and~~ This is another example where our earlier experience in cryptanalysis, particularly with the Red Machine, came into being. What was needed were during this change in wiring between the cycles of each card passing through the machine and being fed into the I think the word is totalizer relays or totalizer accumulators in the tabulator was

TOP SECRET

just a half Hebern. ~~Hebren and~~ Once this became apparent to us, all we had to do was borrow some switches from our stockpile ~~that~~ of spare parts for the Purple Machine just enough to build a commutator. ~~and~~ I remember actually wiring up some of these switches to produc such a ~~accommodate~~ commutator while my younger boy was being born in Georgetown Hospital on a Sunday morning and I was babysitting the older boy. I mention this because I think its important to note we had no facilities for doing these special jobs except to send them to Signal Corps Laboratories, ~~and~~ this would have been impossible to achieve at the time we needed it and we would have lost track of what was happening or to turn to Navy Yard. But the job was so trivial and the kind of a thing that could be done in your home workshop that I chose to do it. However if it had been more complex I guess we would have let a contract and maybe we would have never built the device. Well once we attached or reached the point of attaching the auxilliary device to the tabulator we were confronted with the problem of how to deal with the IBM machine without internal modifications. We fed the commutator from the plugboard plugging out of the normal tabulator plugboard the reading positions from the reading brushes into the commutator and then out of the other side of the commutator into the printing brushes and into the accommulating counters in the machine. The onl

TOP SECRET

reason for going inside the machine was to get an impulse, a cyclin impulse, to advance the commutator one step as each card was passed through the machine. We found the wiring diagram which showed a vacant relay in the machine ~~which~~ that responded to each cycle, so we ran in one pair of wires to the closing contacts of this relay to energize a master relay we had wired from a Purple Machine stockpile, ~~and~~ this relay then controlled all the power that went into the auxilliary device we'd put together to do this wire switching wire changing and we hooked the thing up turned on the tabulator put the deck of cards in and the first run was a succes It just worked almost like magic and from that time on our proble was to modify and make more efficient this technique of modificat of the IBM machines. Now maybe I'm cheating a little bit when I say we modified the IBM machines. We didn't touch that machine excep to borrow ~~that~~ the contact. But the principle was established that we could through even though it was an external modification indirec to the machine if I might use that term. We did modify the use o the accounting machine, ~~that~~ the philosophy of the accounting machine and we did something that just hadn't been done by IBM because th had no reason for doing it before, but it set the stage for a lot of other things that came on and I think its greatest benefit was it proved particularly the people who were dedicated to the manua cryptanalytic approach it proved that there was a new field which was much more fruitful and new techniques which were much more powerful through the development of automatic processes utilizin equipment in unorthodox ways. The device of course pleased us considerably, and it took us only a few days to establish that thi

TOP SECRET

thing really was a breakthrough and without this device, and at that time we in our puckish way gave odd names to things, you remember SUZY Q for the analog of the Purple Machine that was hand operated, well we called this the "Geewhizer." ~~and~~ The name stuck, and I think it is still referred to as the Geewhizer maybe in the literature as well as familiarity is a familiar expression when referred to by people who knew about it in the early days. When the we reached the point of being satisfied that we developed a viable technique, useful and profitable, we of course ~~probably~~ broadly wanted to show it to the Navy people and we brought them in. I think I showed it first to Hargraves, who had provided me with the photographs, and he kind of shook his head about it. He said that's too much trouble and he went back and he talked it over with his people. They had an IBM installation at this time which was dedicated to work on the Japanese in a sort of uncertain way. I say dedicated I think that's the wrong word because the Navy IBM installation was the responsibility of somebody who had to provide IBM support to other activities I believe beyond the group that Hargrave was working with. I think some of the COMSEC responsibilities had to be satisfied by this installation so Hargraves didn't have the easy, open access to the IBM equipment that we had, but in spite of this sort of administrative inhibition, when he brought his associates and they saw how effective this thing was now actually

how effective it was in according us with a rapid solution to these Japanese transposed code system, they of course wanted one like it and we built several models. Each one was a little better than the last. But they all had sort of a haywire look, but I can assure you that they were very positive in their action. Their electromechanical action was just as good as could be achieved by some ham fisted amateurs operating with telephone equipment. All this was done of course without IBM knowledge and when the IBM serviceman had to come in and repair a machine in the installation we had to go and take the plugboard out and pull out the two wires to this relay. Actually we I think we through some subterfuge lost the cover to this IBM tabulator so we didn't have to take it off and put it on each time we installed the machine so that when the service man came in. I think he gave us a few groups on dissatisfaction on this, but it was easier for us to leave the machine uncovered so we could get in to remove the evidence of its being used for purposes not authorized by IBM and anything else. An interesting sideline to this, probably this is a bad place to throw it in. Later, several months later after we had really gone into the routine of using this Geewhizer to solve the daily traffic and actually we got ahead of the problem -- We were able to go into the backlog after the Geewhizer was put into effect and read messages that couldn't have been read by hand techniques under any circumstances. Of course we always did the

TOP SECRET

easy ones first and then left the hard ones as ~~for~~ rainy day problems. That wasn't too bad a problem because the more traffic you had the easier the day's traffic was if there was only four or five messages in a day there were some days like this, particularly Sunday, that you didn't worry too much about the information you ~~xxxxx~~ lost because quantity wise you had the bulk of the traffic already processed. Well the point I was going to make is when Col ~~Bridle~~ Verkuyl came to join us he was reputed to be the greatest cryptanalyst ever produced by the Dutch the Netherlands government and that he had been successful in reading Japanese messages. Well it turned out that ~~Bridle had~~ Verkuyl and his group had been employing on this Japanese transposed the technique which were identical to the ones ~~Fahvan~~ Feinvin, the Frenchman, had developed for the ADFGVX, namely the similar beginnings and ending I remember him explaining to us exactly how he achieved this solution, ~~and~~ we of course were right on top of it because he had gone only a small way down the manual process that we had completely followed and so we were far ahead of him. Finally after some deliberation as to whether or not we should let him in on the Geewhizer because he just couldn't understand how this small force that he'd seen were able to read all the traffic that we had read and the tremendous number of keys that had been produced. We hadn't told him about the technique but we'd shown him the results. He just couldn't believe it and finally when we showed him the Geewhizer he was a most awestruck individual. We were so far ahead of the point they had reached that it was it was really unbelievable to him.

I'm a little hazy right now in my recollection as to what our identification for the systems used by the Japanese diplomatic communicators the transposed system we were processing by means of the Geewhizer, just what its designation was but it seems to me like it might be about J16, 17,18, and 19. This of course will become clearer if we look at the description, technical description of the systems and you can identify precisely which systems are involved, but I think if you look around 17, 18, 19 "Js" of course in the Army terminology you can identify these. Now all this story which I've told about the development of the Geewhizer, the essential parts of it are included in an article which was published in the technical journal, and since that article is not signed there may be some mystery about it. I think I ought to explain where the article came from. After we had put the Geewhizer together, Friedman was quite impressed with the achievement and actually ordered me to have a report written up describing the device and how it should be operated. We were inhibited though in my meeting Friedman's requirements. The reason he ordered me is because I was very dilatory about writing up technical things and I hoped somebody else would do it. ~~and~~ It wasn't because I didn't think it ought to be written up its just that I didn't feel like I could do it at that time. But we were inhibited by another thing and that was the security implications of such a write-up. Friedman's desire was to have

TOP SECRET

this technique written up so that it could be [redacted] generally used for the training of our new cryptanalytic force, and at the same time we didn't want to reveal to them that the thing had been generated in its application on the Japanese problem. And it was particularly sensitive because the second-story operation that had been performed by the Navy to produce us with the first set of keys and codebooks that we exploited. So as a result of this the ~~writeup~~ write-up ~~that~~ which was prepared on this GEE was pretty much sanitized and the device was described, I'm sorry the Geewhizer the device was described, in terms of a made-up problem. I don't think the made-up problem is near as dramatic as the actual circumstances, and I would like to bridge the gap between the ~~writeup~~ write-up which appears in the technical journal. ~~and~~ The reason it appeared there, as I recall when I was publisher of the Journal, Bob ~~Brogman~~ Brockmann, who was its editor, reported once that he had a dearth of articles for the Journal and we agreed that we would go back and print some of the old historical ~~writeups~~ write-ups including not just the Geewhizer, I remember two others, the one on the Purple Machine was published without attribution and another on the German one-time pads system, the GEE system which I think in itse probably one of the most startling cryptanalytic developments tha I saw in my whole career. And I might mention here just because it might not be recorded ~~anywhere~~ place else that we didn't really solve a one-time pad system as John Tiltman refers to in "The ~~Forward~~ Foreword" in describing some of the problems which were generated

TOP SECRET

TOP SECRET

by this work, but we ~~saw~~ solved the mechanical device ~~as a~~ process by which the one-time pads were generated, and if they ~~were~~ been properly generated or a better machine had been used for the generation of course the GEE would not solution would not have been ~~obtained~~ attained so in essence the solution of the German one-time pad system was the solution of a form of cipher machine.

End of Side 1

Side 2 of Tape 10 is blank

TOP SECRET

Tape 11, Side 1

TOP SECRET

Q: What effect did the advent of the electromechanical cipher machine such as the Red, Purple, Enigma and SIGABA have on the state of the art in cryptography?

A: ~~Mostly~~ Grossly from my viewpoint these represent the first practical application of electromechanical principles to be used in the code ~~books~~ rooms. Now the earlier models were not the most perfect machines in the world but they were quite adequate. The material the state of the art of construction of this type of device had not reached the point where the machines were totally reliable. Consequently the earlier models ~~have~~ gave a lot of maintenance problems to the users and to the people who had to keep the code room running. But these were much less than the onerous task of running the messages through a two-part code with a hand encipherment and also had the advantage particularly in the case of the Red and Purple and the ABA, not so much the Enigma of printing out the plain language so it could be presented immediately to the fellow who was going to receive the message if you so desired. ~~They~~ We got a little closer to real time in the use of these devices which was probably the greatest advantage from the user standpoint. From the code production standpoint the people who prepared the systems and the materials that go out to the code rooms there was a considerable advantage because in the case of the ABA we could use those wheels to store a tremendous amount of key which consumed only a small volume less than a fourth of a drawer in a file cabinet or a safe whereas the literal keys or manual keys used with the old code books like the M110 the 11 as we visua-

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

the War Department staff code, the War Department confidential code, would have had to be changed frequently and would have been voluminous in that it would have required considerable storage space and been a real pain for transport to the more distant posting stations where they were held, particularly the military attache systems because couriers sometimes very infrequently got to some of the more remote posts and stations. Now these were the advantages that were immediately recognized so far as the electromechanical devices were concerned and I think we can look at the development of these sort of like steps and stairs with each machine you climbed higher. You took another step toward improved security. Now the other side of the question is what about the effect of the development of these stairstep-like devices as I just now described. What did it have on cryptanalys Well you never know how to solve a problem. I'll pontificate a little bit until the problem has been defined and as each new machine came along with its improvements we defined new problems in cryptanalysis. Therefore we were able to direct our attention, mathematical and statistical and the other types of analysis that we had begun to develop and appreciate at each one of these improvements. In due course we achieved solutions to many of the cryptanalytic problems presented by the improvements as they appeared as new inventions came out in these devices. Basicall until the aftermath of WWII we depended largely on the electro-

mechanical devices and mechanisms for our mechanical enciphering process. After that of course the state of the art permitted us to go into electronics, and I would like to limit my remarks about both cryptography and cryptanalysis to the electromechanical phase because I think, while you could generally say the same concept would apply to the electronic, it would be better to define it in terms of what actually happened in the electronic phase of cryptography.

Sammy, how far did I get off the beam on this please sir?
(You got right into the problem, but I would say just started to touch on the cryptanalytic aspects as how did these developments affect our cryptanalytic efforts, and I believe we could add a bit about the what we learned because of the weaknesses inherent in the design of the Red system especially and a little bit in the Purple as well as administrative errors in such that the enemy made. We learned a number of things not to do, so to speak, and this was particularly glaring in the difference in the kind of wheel that was used in the Red and the tremendously more powerful type of thing they had when they went to Purple and even there its weaknesses too taught us a lot.)

We've been directing our at least I have been directing my remarks and I think Sammy also had in mind the theoretical considerations the overall considerations but there were certain practical advantages which developed from our work in the exploitation of the Red and Purple machines that the Japanese were using. This gave us a wonderful opportunity first-hand to observe the advantages which the cryptanalysts ourselves could obtain from poor training of code clerks, poor xxxxxxxcode room procedures

TOP SECRET

and generally misjudgments in the type of cryptography that would be used and once we started to identify these weaknesses and were able to exploit them then it put us on the alert that these were the kind of things that we should avoid in our own coderooms, and so we tended to fold back the results of our experience from work on the Red and the Purple specifically into our own coderoom procedures and eliminate some of the bad practices that might have developed and certainly would have been followed if we'd left the coderooms alone. Probably another important aspect of this was it taught us that we had to be alert to almost continuous monitoring of all of the messages that went over the more important circuits and certainly when we introduced a new system, a new machine, a modification of the ABA or something like that we found that we ought to monitor its use particularly in the early months of its life to insure that the coderoom people were not doing something that would undermine the security of the system, and this I think was a particularly important lesson that we learned We just didn't trust our own systems, and as we watched the Japs use the Red and Purple, now we realized that this fear was well founded and that we should be on the alert in all the months of the use of a system. From this sort of experience grew our wartime conviction that we had to have a monitoring, we had to establish and provide for the monitoring of our own communicatio

That was impossible to do the thing totally, but we were able to effect a small sampling of the wartime radio transmissions and study these. We had a unit set up whose purpose was just to study these messages that had been intercepted and look for cryptographic mistakes as well as the kind of things that you would take advantage of in traffic analysis and the like. ~~in the line.~~

(Remarks made by Sam Snyder)

An example of the inherent weaknesses that enabled us to get into Red relatively easily and then Purple with ~~was~~ a bit more difficulty were the design weaknesses of the nature of the system itself. In the case of the Red machine I think the kind of wheel they use the Japs must have thought it was great stuff and it turned out to be just the opposite. I think we call that type of motion that type of encipherment half Heberm ~~Hebron~~ rather than having a comple scrambling possible on each side of the wheel so to speak. Let's see, other examples of weaknesses depend a bit on the motion or th limitations, either the limitations built into the machine or the limitations or weaknesses due to the way they were used. In other words the latter, if you just changed a rule or two about how to use starting settings, daily changes and so forth could make a huge difference in security and all of these turn out to contribu and make a big difference in how we are able to read these. ~~and~~ Again each time we learned something about cryptography of the other system we learned what not to do or what to watch out for in our own.

A: Sammy, one thing I'd like to add to what you said that's very important. In both the Red and the Purple the Japs made terrible mistake from the standpoint of secure cryptography of dividing

the 26 letters of the alphabet into two sub-sets, ~~6s~~ "sixes" and "twenties" 20s. Now in the case of the Red, and I think this story is told elsewhe in our tapes, we took advantage of this stupid thing the Japs did in cryptography by solving first the "sixes" to the short sequence and, when that was recovered it enabled us rapidly to recover the "twenties." Again this goes to the old analogy of the fascine where if you can divide the problem into little parts it breaks up easier. Well the Japs automatically divided the problem up into little parts by giving us the "sixes" and "twenties." Now I think in terms of the state of the art in our experience that we might not have solved the Purple had the Japs not employed this "six" and "twenty" division because the real thrust of our effort on the Purple Machine was to recover the "sixes" which the Japs sort of took for granted would not provide a weakness represent a weakness in their system. But once we discovered how the "sixes" operated and were able to decipher and we could decipher every appearance of one of the "six" characters in any message that we intercepted after about three months of our effort we had in many cases where the "sixes" represented the most frequent letters of the alphabet we had as much as 15 to 20, 25% of the text of the messages presented to us simply because they chose the "sixes." Of course this lead us to the next step of guessing the what the "twenties" were, and It was pretty straightforward approach. and We first had to accumulate enough data then to cover the more complex and more sophisticated maze which was used for the encipherment of the "twentie and There the Japs pulled a little dirty trick on us because

they used a very simple form of the "sixes" and they complicated the "twenties" by running them through three separate mazes I'll use this term because I think it describes it in cascade whereas the "sixes" had only one substitution maze.

Q: Frank, that reminds me (S.Snyder) of just another point that comes under the heading of lessons and so forth, but in a broader sense. What the Japs were doing in not only these systems that we have been talking about, but we saw it in other systems was gradually improve their security or sometimes they weren't improving it, but each time they made a change there was a gradual change or they kept as a holdover in a new system some feature or some characteristic of the old which enabled us to keep up. As long as we were keeping current we were able to add to our arsenal the same kind of tricks. Now when the main lesson I'm referring to is that when you make a change you should make it a complete change to utterly entirely different kind of a system. ~~and~~ One other aspect of this gradualness was that they even signaled the changes by sending in messages I mean in their messages that we were reading the notice of the next change which is a kind of an obvious stupidity but gradualism and notification was another aspect of the weaknesses and lessons learned.

A: To make ~~but~~ this discussion real may ~~and~~ I recall where we took advantage of the lessons we learned from the Japanese. Both of these came out of the work on the Purple and I think the first of them is the more trival of the two. We learned that by breaking the message in the middle and sending the latter part first with the end buried somewhere in the middle and then the beginning

of the message later on, we avoided certain weaknesses of having beginnings which could be assumed because our greatest work on -- our greatest results from the Japanese was our ability to guess the beginning of the message. I have written in and I'm not bragging because other people have done this too as much as 50 or 60 and sometimes 150 letters of accurately assumed plaintext at the beginning of a message, and Once you've got this kind of a powerful opening into a thing it takes a pretty doggone system to stand up under it. Now while we rather suspected that this was a weakness that might be applied to our own systems, the work on the Japanese and the advantage which accrued to us by our ability to guess the beginning of the message caused us then to introduce what we call the "Australian Crawl" in some of our messages which was first used between Brisbane the headquarters there, Akin and the Signal Corps people down there and Washington headquarters, where we actually bisected the message following the practice used by the Japanese. So here's a practical example of a lesson which we learned from our work on the Japanese Purple.

Q: (Snyder) This bisection of messages to avoid stereotype beginnings was later adopted by the Japanese and used in many of their systems, and I particularly remember that it was true during the war and Jap army systems and some others.

A: Now I also recall another somewhat less direct result of our work on Japanese which was used to advantage in our own COMSEC work. One of our problems in recovering the Purple keys was to determine the actual assortment of letters in the "sixes" and "twenties"

because they changed this arrangement daily. In other words each day we had to derive a new set of "sixes" and a new set of ~~xxxxxx~~ "twenties." The way we did this was to take the indicator for the particular message we were studying, try to guess the beginning, and then by examining the relationships of the plaintex letters with the cipher text letters through the various encipherments provided by the machine at this particular indicator setting — recover the identity of the letters and their location in each of these sequences. This was pretty handy way of doing it and while it sounds very simple sometimes could be a pretty hard thin to do. Now in our first work on this we used to use the cipher machines which was a clumsy sort of slow process, ~~and~~ we had two machines, the automatic machine we had a spare we used for crypt-analytic purposes ~~and~~ then we had the old hand model which we called we had a pet name for it, I think it was Annie, and she was a very stubborn lady to deal with because pulling those bars across with the twenty contacts down the board was almost impossible for some of the girls to do and thats — —

Q: (Wasn't that called the SUSIE Q? That particular one with the bars?)

(Snyder) Frank, excuse the interruption but didn't we call that sliding bar hand tested device for the Purple the "twenties" the SUSIE Q rather than Annie?

A: Sammy, you're right. I think I was thinking more of Annie Barker who was one of the young ladies that protested the use of this thing because we teased Annie about the device and I think we called it something like Annie's Delight or Annie's Toy because she hated i so. But you're exactly right it was the SUSIE Q and I think we

formally
~~finally~~ called it this even though some of the girls hated it
sin
and I don't blame them for it. So that we didn't have to use these two somewhat clumsy and certainly inefficient ways of determining just what the connections were in the machine when we were recovering the sequences for an unknown key, we produced what we call "Development Sheets". Now the way these were originally produced was for Mrs. Jerome to sit down at the cipher machine, set the wheels up at the first position given by the indicator and then type out the complete alphabet from A to Z. Then she advanced the cipher mechanism to the second position provided by the indicator and again typed out the complete alphabet in the same order from A to Z and so on until we had produced about 150 positions of the settings of the machine for a given indicator. Now by using these tabulations we called them "Development Sheets" and I don't know what the logic of this term was. The girls could recover the keys a lot easier than by using SUSIE Q or the device itself. Well Mrs. Jerome was a very much overworked lady and so one of the cleverest things that I think we did in those days is take one of our cipher machines, the Purple machine, ~~and get in~~ in good working order, and plug it into an IBM tabulator and automatically cause the tabulator with its cards to advance the machine and with each position of the Purple machine we would read the entire bank of the letters of the alphabet so instead of taking something like probably half a day or maybe a full day to produce a development sheet, or a set

TOP SECRET

of development sheets, we could run off a whole cottonpicking thing in a matter of five or ten minutes and then set up the machine and do the second one, and we produced a number of these books which we passed around to the cryptanalysts who were recovering the sequences for each day and enjoy this advantage in ~~laborsaving.~~ labor-saving. Now that's what we did cryptanalytically. Later on ~~when~~ the Navy was confronted with the problem of producing a tremendous number of mixed alphabets and what they did was to take a couple of ABAs, and using exactly the same principle that we had followed in connecting the Purple machine with the tabulator, they generated these alphabets by the same process using wired rotors in our own machines and were able therefore to cut back on the code production program satisfying both the cryptographic security problem which they could analyze. We knew a lot about rotors and their secure properties and their insecure properties so we could go into the use of these alphabets with a certain reassurance that they had already achieved, represented an adequate level of security and save ourselves a lot of theoretical research. This went on I think we used it in the Army too, I believe that's where the Navy encountered it, the Navy COMSEC people because we'd used it for development of certain key lists and we thought about using it for a generation of a alphabets for the M138 strips. I think this was not only a practical trick but I think one of the cutest tricks that we did in those days because nobody had ever thought of hooking up a cipher machine to a tabulator and running all 26 letters through it before.

[redacted]

Q: (Snyder) Frank speaking of developing tricks this isn't to go too deep int the solution process of the Purple but to bring about another one of those lessons that we were referring to earlier. Do you remember in the last ~~xxxx~~ few months of this exploitation of the Purple, you believe developed to a very fine point the list of indicators and settings and finally we had this so that we could generate the alphabets in advance, ~~and~~ so we had future and predict alphabets and settings because the key or the nature of the relationships from day to day or from month to month were solved, and we were able to have in advance the settings before the Japar arrived which is another of course points up another lesson for us about being too systematic.

A: May I elaborate on that a little bit? You're indeed correct abou our ability to predict the keys using the Purple machine. You're incorrect in your attribution of this discovery to one Frank Rowl I did not do it, But the way it came about was this. When we saw that the Red machine years before, several years before, I was lucky enough to discover there was a relationship between the sequences lc used for the Red Machine and as a result of this observation we were able to predict in advance all the keys used by the Japanese lc for a period of about almost two years. That's Red Machine keys, ~~and~~ The reason we were able to do this is that the Japs had devised a way of replugging the board using one basic sequence in generating from it a series of sequences simply by moving the plugs ~~in the~~ between the cipher machine and the printing device and the typewriter keyboard. We used to puzzle about this because every now and then we'd find a mistake ~~in the sequence~~ where a couple of

letters were interchanged, and there would be some kind of a message coming out from the Japanese foreign office in Tokyo making remarks about ~~the Sosan~~ SOSAN which we never quite understood because nobody ever knew what a ~~Sosan~~ SOSAN was. There wasn't any such thing in the dictionary that seemed to describe the part of the cipher machines ~~xxx~~ that was being referred to in these messages. Still a mystery to me but this ~~Sosan~~ SOSAN thing which I throw in sort of as a curiosity evidently was a descriptive term they use for replugging the plugboard, so that they could use one sequence to generate a number of sequences. Now after we solved the Purple and it had been in use for several months I believe Mary Jo Dunning and ~~Jean Finstein~~ Gene Feinstein discovered a similar property in the Purple keys, ~~and~~ From that once having noticed th and done some work on it Miss Dunning and Mrs. ~~Finstein~~ Feinstein in collaboration with others of the staff and I guess Sammy we might have been involved in this as well as Furner and Small and also Raven and the people over at the Navy because we had a complete exchange of information and once this phenomenon had been observed then we all tried to contribute to removing the mystifying aspects from it. So you're exactly right Sammy. We did do this except I didn't do it for the ~~purpose.~~ Purple. -- I think This is a little off the subject of security but it goes while Sammy and I are together we can compare notes on one of the most critical points in the solution of the Purple. ~~and~~ That was when we found first the evidence that we had been hoping to find

which assured us of certainty of success in recovery of the Purpl machine. ~~The~~ As I recall it was like this and Sammy please check me. Three or four of us I believe I don't remember whether it was you and Furner and Small and myself were in one of the work rooms but I think thats what it would have been when sort of havi a gab fest on what we had seen and other things to do and at that time the whole work force was involved in searching for a certain phenomenon that we expected would result from a machine of the concept that we had evolved for the Purple enciphering mechanism. Now we had recovered by this time the plaintext for a great number of messages, ~~and~~ The problem was to search through these messages for a particular phenomenon which we had identifie grossly but had to be identified finally by discovery. So we ~~wre~~ were looking for this phenomenon without actually being aware of precisely what we were seeking. We knew the effects we were seeking rather than the specifics of the letter, ~~of~~ or what diagraphs to search, so it was not a thing we could run through the IBM machines just a little bit too sophisticated or complex for them to deal with. Now the workload had been divided up and one of the working tasks had been given to ~~Jean Finstein~~ Gene Feinstein nee ~~Jean~~ Gene Grotjan Groche who was a very, very capable cryptanalyst and very observing and very reliable in her analytic work. Now I remember we were sitting a few of us, I guess Sammy and Al and Bob Furner and myse discussing some aspects of our work when ~~Jean Finstein~~ Gene Feinstein came in -- sort of timidly as was her custom and with her worksheets sort of clutched to her bosom and sort of politely waited until she found

TOP SECRET

an opportunity to interrupt us. ~~and~~ When she said, "Excuse me, I have something to show you," We all sort of broke up our ~~business~~ meeting and invited her to spread out her worksheets on the table. ~~and~~ She took her pencil and after laying her worksheets out to suit her requirements said, "Please look at this," and pointed at specific points on one of the worksheets, and "how it matches this on the second worksheet, and its over here on this on the third worksheet," and we all looked, and there was no question. She had found that first example of the kind of thing we'd been searching for many days for. At that point when we saw this I don't think anyone of us had to tell the other what it meant because we knew we were well enough along in our cryptanalytic understanding of the problem to know exactly what this meant. ~~and~~ This was the actual breaking point from where we were uncertain that we could read the cipher we were hoping -- we felt pretty certain. But ~~that~~ when Gene ~~Finstein~~ Feinstein brought in these worksheets and pointed out these particular things we knew that we were into the Purple machine and that it would be solved. ~~and~~ As a result of this the rest of the team went and pretty soon we began to find other evidence and after accumulating enough of this we then were able to start recovery actual recovery of the wiring of the mazes.

Just to clarify the roles of some of us. I've mentioned Feinstein, ~~Finstein~~, Turner, Small, Snyder, Rowlett, Friedman and Rosen. ~~Me~~ I don't intend to leave out Sinkov, Kullback and the other members of the staff at that time. I've been talking about those who were assigned at that instant to the Japanese problem. ~~and~~ I might

~~TOP SECRET~~ TOP SECRET

talk a little bit about how the organization developed. We started, as a first priority, working on Japanese. Once we got to the point where we could turn out translations, and a little bit later on establish that we could read all the Japanese diplomatic messages in their best system there was no stopping the growth of the Japanese diplomatic group because G-2 would have objected if the Chief Signal Officer had cut it back, and we weren't about to anyhow because it was too exciting an operation for us to let suffer, But there was also pressure to develop work on the German and Italian which were the second and third priorities, and probably because I had not taken an overseas assignment and was so deeply involved in the Japanese I inherited it. Kully and Abe respectively were given the jobs of organizing what we hoped would be a similarly successful effort on the German and the Italian, and Abe also inherited sort of the rest of the world like French, Spanish. We called it the Romance Language Section because the staff which was assigned to it was competent, well, anybody who can speak Italian, Spanish can speak French and vice versa, sort of. German was a little different and Japanese was certainly different because the uniqueness of the Japanese language. Now the lines weren't too closely drawn in the assignment of personnel. I remember one of Mr. Friedman's problems was to act like Solomon and divide the children among the three sections that I've mentioned, and We couldn't, he just absolutely couldn't set up hard and fast rules about the assignment of individuals because if there was a urgent problem which required a lot of effort in the German or the Japanese or the Italian then provisi had to be made for the reassignment of personnel or the loan of

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

TOP SECRET

personnel or the shifting of personnel from one of the basic ~~div~~ divisions to the other. Actually the division of effort was more a guidel for us to follow and as I'm sure is the case today we had to establish certain responsibilities for the personnel and hang them on some kind of administrative peg, ~~and~~ I think the organization was more one in response to administrative requirements than it was problem requirements because the problem requirements were looked at as very fluid situation and adjustments made even for half days or hours at a time, by shifting one person from another from one job to another, ~~and~~ also we had the main support facility which was our accounting machine installation which had to be staffed and it was supporting all three sections that I mentioned as well as it could. It was understaffed, ~~and~~ I think Sammy you will remember that you were spending a lot of time as a machine room operator because there wasn't anybody else there, and I'm sure Al Small did. Furner never got stuck with this as much as others althoug he was willing. You and Al certainly doubled many times in bras simply because there wasn't anybody else to do the run that was required for -- whether it was the Italian or the German or the Japanese outfit. One of the interesting developments that our work on the Japanese system in particular because the main information, high-level ~~highlevel~~ stuf that G-2 ~~G2~~ was interested in and Japanese went with ~~in~~ machine systems, If the message was addressed to the holders of the machine. If it was not addressed to the holders of the machine it went in a special code -- superenciphered usually with a transposition system It was typical Japanese code superenciphered with what they considered a very secure system. There were a variety of these.

~~HANDLE VIA COMINT CHANNELS ONLY~~

TOP SECRET

TOP SECRET

They started out pretty simple and they went to more complex forms ~~one~~ until we got into the type of transposition which was cryptographically patterned, although I don't know whether the Japanese realized it or not, cryptographically patterned after the old ADFGVX Army field cipher system used in WWI. ~~and~~ This latter was pretty nice to challenge to us and resulted in probably one of the most significant achievements that I recall as a breakthrough in the application of equipment, accounting equipment, to cryptography and I think opened the door to computery. But set that aside for the minute. We found that the Japanese problem afforded us the best training ground for the development of a comprehension of cryptanalytic principles as they could be applied to the cipher machine and the machine solution, ~~and~~ It's ~~was~~ my conviction even today, and it was all along that it took a much broader, ~~and~~ a much more advanced posture in cryptanalysis to deal with machine problems than with the old hand systems into which I will dump the additive type. Now I may be unkind to some of my old friends and co-workers by making this differentiation but the principles of additive recovery were basically simple, ~~and~~ I think if you knew how to make the difference table and apply it, this is all you needed to know to be successful as an additive recoverer. But if you were going to do what Gene Feinstein ~~Jean Finstein~~ did and discover this sort of suspected but still unidentified attribute without ~~xxxxxxx~~ the ~~xxxxxxxxx~~ benefit of difference table or experience before you took it, an entirely different type of approach, a different type of training and a different type of attitude to be successful And this you developed only after months of experience and considerable intensive training and the more advanced analytical aspects of

~~HANDLE VIA COMINT CHANNELS ONLY~~
TOP SECRET
~~TOP SECRET~~

cryptography, well cryptanalysis really. Cryptography is in this instance is subordinated to cryptanalysis. So our workforce had to was an entirely different breed of cryptanalysts and what you encountered and I apologize for my friends in England and the Navy when it just came to recovering additives. Now Kully and Abe had a lot of this additive recovery to do so I'm not going to downgrade our attitude towards additive recovery because some of the work they did, particularly in the Floradora where the we called it the two-time additive, the reuse was extremely sophisticated and Kully had a field day in his application of statistics to this kind of a problem because he refined the old sort of simple minded difference table concept. He and his people until it was a much, much more powerful cryptanalytic tool than I think had ever been applied before. So to summarize a little bit, our experience with machine cipher and our success in machine cryptanalysis developed a whole new breed of cryptanalysts which the world had never seen before. I think in our case we had an advanced position even beyond that which I found when we went to Britain where they had successfully exploited the Enigma. I think our understanding of the principles underlying the Enigma solution was at least as good if not better than that arrived at by the specialists in GCHQ who developed the Bombe. And this was because we had tried to work out well we had successfully worked out the Purple, and we'd been deeply concerned in the development of such things as our own cipher machines and both the Navy and the Army had joined forces in this. We therefore had a much better view of machine cryptanalysis than I think anybody else in the world at that time.

HANDLE VIA COMINT CHANNELS ONLY

Tape 12, Side 1

[redacted]

Before the attack on Pearl Harbor there were several SIS intercep operators and a intercept detachment or unit, I don't know what the formal name was but there were quite a few of our intercept boys operating in the Philippines. Their primary mission was to try to pick up any Japanese military messages that they could ~~xxx~~finc I might point out that before Pearl Harbor, as I recollect, there was only a very small amount of Japanese military that we were able to intercept. ~~and~~ We had a great hunger to get as much of that as we could because we needed a broad base of intercept for us to start our cryptanalytic attack on the Japanese military system, particularly the field systems. About ~~XXXX~~ all we knew about them was based on some of the earlier ~~area~~ research which we'd done on the meager volume of intercepts we'd received -- some of these were taken in the Philippines, so the unit was not just a thing which was established immediately before Pearl Harbor or hostilities broke out, but one of rather long standing. We had admired greatly the Navy's intercept capability in the Far East. I think it was one of the best I have ever seen. I've got to say some words of pra about the US Navy intercept service, ~~and~~ their coverage of the far eastern diplomatic net, and naval circuits, Japanese naval circuits, and naval traffic in the Far East I think was a brilliar job. Also the Navy as sort of a contrast with the Army was undertaking considerable processing of intercepted material. ~~and~~ I'm sure while I'm not fully aware of just what they were doing in the Navy I'm sure they had quite an effort directed at Japanes naval communications, and they ~~wre~~ were doing some processing of the diplomatic. I vaguely [redacted] picked out a machine, a

[redacted]

~~TOP SECRET~~

Purple machine to send out there, but I wouldn't swear that they did have it based on my own recollection but I'm sure the records will show I believe they had it. This morning I don't remember that much detail. Now what did the small units of army the SIS unit have for its mission. Its mission was to do intercept search for Japanese military. To intercept what traffic they could to satisfy the requirements or to help to satisfy the requirements of the headquarters activity in Washington. Our interest was Japanese diplomatic and there was a great interest in finding out and receiving rapidly information about the Japanese activities in the Far East as reflected through decodings and decipherments of messages that went over the Far Eastern dip net. This was very high priority although the highest priority at that time was to keep Mr. Roosevelt personally provided with the translations of messages between ~~of messages between~~ Oshima and Kurusu in Washington and the Japanese foreign office in Tokyo. Now ~~when~~ after Pearl Harbor some rather interesting things took place, and thats why I wanted to put my answer to the question on tape because I don't recall having discussed this before in terms of history.

The unit in Corregidor was in constant communications with Washington. Constant in the sense that we had traffic, great volume of traffic coming in, because it was extremely difficult to get this traffic out any other way except by radio, ~~and~~ so we'd set up an M134, I believe it was one of the earlier models of the M134, both in Corregidor

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

and the area which had been assigned to the Signal Intelligence Service and in our own area in Washington where we decoded the messages which had been encoded in Corregidor, intercept messages and we processed these rather immediately. I remember looking over the decodes as they came in. The most interesting message that I think I've ever read in my life came in that batch because when they had finished the encipherment of the intercept messages and completed their business, the one of the operators would sit down and type up his observations his reactions to what was happening during these last hours before the fall of Corregidor and some of these messages would just break your heart when you read them. I remember them talking about the despondency they had "~~xxxx~~ It can be only a few hours now." One of the boys said "How I would like to have a fried chicken dinner." or something like that. It was right pathetic. The intercept that we got in those last hours, though unfortunately for the record wasn't too significant. There was no great gems in it. Of course this was now some months some weeks after Pearl Harbor after the attack The effort tapered from about December 7 down through until the fall of Corregidor which I believe was a little nearly spring of well a little earlier than May, according to my recollection, but history will show what day it was.

I don't recall specifically if there were instructions to Gen. MacArthur from Washington to evacuate the Signal Intelligence Service troops from Corregidor. I recall dimly some stories about the last days. I recall that Akin was reluctant to leave his men. He was a damn good commander, very loyal to his troops. There

~~TOP SECRET~~

was one story that when the Japs were pressing on the back driving the Americans, a small group five or six of his men -- Signal Intelligence people got caught in a ravine and trapped by the Japs. ~~and~~ Akin personally took a machine gun -- a tommy gun and sprayed the understanding brush on the other side of the ravine ~~standing~~ out exposed so he could get a good view ~~of~~ a good perspective of the other side and I guess caused the Japs to go to cover so his men could run across this bridge and come back to safety. Now his loyalty to his troops was almost a legend in that time and I have heard, and I couldn't prove this, that MacArthur ordered Akin personally to go with him and that's the only reason Akin left. He couldn't refuse an order, but he didn't want to go and leave his men. So I would assume that this is what happened somewhat as follows. That there were plans -- yes, there were plans to evacuate every American but the facilities and the opportunities for evacuation were so limited that only MacArthur and the top level of his staff including Spencer Akin who was his Chief Signal Officer at that time could be effected. There just wasn't enough to take out everybody. Now a lot of the boys were on the BATAAN Death March, ~~and~~ Art Peterson who survived that march and who was later on the SIGINT business and deeply involved in the drafting of the consolidation orders and papers told me of a couple of our boys that I personally know who'd been trained in Washington and of their fate. They lost their lives as a result of this death march. I don't think there were too many of them ~~that were~~ involved in the death march but I don't think we'll ever know what happened to some of those boys.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

TOP SECRET

So far as direct support was concerned in those days, before Pearl Harbor we hadn't really been able to do much. We had some war plans sort of indefinite in nature but generally that we would have forward processing and intercept for field systems somewhat patterned after the WWI ADFGVX type of thing and plaintext intercept which would be immediately available. I think we called it Radio Intelligence Companies and if you look into the record of history the RI Companies you'll probably get a pretty good insight into just exactly what happened, the effectiveness of these companies, their strength and the progress that was made in assembling them. But the first real thrust at low-level processing or front line processing, front echelon processing came in Europe when George Bicher went over (Col George Bicher who was one of our signal intelligence students, officers assigne to the SIS training school). He took a two-year course of duty where he was trained as a cryptanalyst, took about the same training course that Abe, Kully and myself were subjected to when we came in, and he was pretty good in this business. So he was selected and organized some RI work to be conducted in th European theatre, and he had his headquarters in London on Wimpol Street just a few doors from the famous house, the Barretts of Wimpole Street, and we used to pass by there when I took a short visit over to the ETO just before D-Day, invasion day, because h was all set up to jump off his RI companies in support of the Allied forces if the invasion of Normandy, invasion was going to be successful, so his companies were going to be in being. They were

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

over there and they did a terrific amount of work. I got involve because he was trying to get his cryptanalytic units trained. We went over very carefully and reviewed the ADFGVX attack and updated our current we did this because if was a terrifically goo thing as a disciplinary action in training the cryptanalysts assigned to the RI company that. the reasons I got hooked in he had nobody on board who knew how this ADFGVX was solved and he took advantage of my being there so I could conduct a few courses in this particular thing, feeling that it was importan for them to know as much as they could about German, cryptography even though that system was not being used. We also reviewe the cryptanalytic work that was being done and they had been trained in on the WWII current German systems which I believe the (17.) Rasterschlüssel comes to me. It was a pretty tough cipher to break and his cryptanalysts had been trained in this. We reviewed the work on that hopefully to see if I could make any contribution, but the work that had been done at GCHQ was so terrific all I could do was to admire it.

The WWII German systems were much more sophisticated than we expected them to be because we thought they might be a great deal like the ADFGVX. But actually I think the Rasterschlüssel was the front line type of system which as I recollect was a sort of a grille applied over it was a form of transposition but it was applied over a code book. It was more like the J19 series

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

TOP SECRET

which was the encipherment, superencipherment of a code and the Kasterschlüssel as I recall used some kind of a code chart. I'm real fuzzy on it. Most of the German army information that we intercepted of course at the upper echelons was in the Enigma and there was no hope that an RI company would be privy to processing of the Enigma traffic. That was too tightly held. So I think the RI companies were, well, Bicher avoided any actions which would get him and his front line processing activities involve in the Enigma type of thing.

Our attitude about second-story operations, that is to request the FBI or military intelligence to steal some Japanese military attache codes, if you will, or Japanese diplomatic codes was conditioned by our sort of proud concept that the Japs couldn't produce a system which we couldn't solve. Now there were two reasons probably which prevented us from taking any positive action over and above our own conviction that we just didn't need that kind of stuff. In the first place, G-2 had no capability whatsoever to conduct successfully surreptitious entry operations. Second the FBI we just didn't want to get involved with them and have them steal codes or enter a consulate because we didn't want to get the Japanese nervous and have them change their other cryptographic systems. So don't be surprised that the Army didn't endorse any surreptitious entry or request any surreptitious entry and I could if you'll take my word for it I heard Gen Mauborgne that he wanted no speak forcefully to ONI and the CNO, Navy heavy-handed, surreptitious entry types to fool around the Japanese

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

Embassy where the Purple or the Red machines or the J19 stuff was, and don't bring us any more pictures of Japanese code transposition systems because we can do it, and if we get the Japs nervous you'll do two things, gentlemen. You'll slow up our success and you will deny ONI and G-2 intelligence because the Japs will change their systems as sure as I'm sitting here telli you about it.

One of the systems or successes that we achieved as the SIS was the work done on the German one-time pad system called GEE. There is an article on this that was published in one of the technical journals that Bob Brockman put out when I was publishe of the magazine and he was editor, and the reason this GEE article is in there is because we thought it might be useful and informative, at least to the workforce, to make available to them some of the write-ups of how secure systems were effectively solved. Of course there's something to a cryptanalyst pretty romantic about the solution of a one-time pad system because so many people have assumed that a one-time pad just cannot be read and rightly so provided you put the caveat that if the pad is properly construc Now in the case of the German one-time pad system we were able to solve it because it wasn't a true one-time pad. The Germans had invented a machine to generate one-time pads and we solved t operation of the machine and thats how we were able to read Germ one-time pad messages. The sort of practical background to the GEE article I referred to is as follows:

Before the war the Signal Intelligence Service was grossly divided into the intercept activity and the cryptanalytic activity

HANDLE VIA COMINT CHANNELS ONLY
TOP SECRET

in Washington and the cryptanalytic activity in Washington was directed at the Japanese which I was the head, German - Kully was running that and Abe had Italian and a lot of other things including French and Spanish and whatever the South American countries that we could get enough traffic on to analyze. Kully's effort was considerable they had done some magnificent work on the system known as Floradora. I don't recall at this point the trigraph applied to it, but we call this a two-time additive. It actually involved a large supply of keys in the form of a key book, and then two separate lines of key were selected by the code clerk and these were added to the numerical equivalents resulting from the encodement of a message. The German plaintext was looked in a numerical type of code and then the numerical code equivalents were written down, two lines of additive were then applied to the plain code text which resulted in a cipher text. This cipher text was then transmitted, and each message had an indicator, a literal indicator which gave the lines to be used so that the decipher code clerk could remove the superencipherment and decode the message of course. Kully's unit was well on in their work on this Floradora and I think he is the one who should tell the story of that so, they were well on it when we started collaboration with the British and I think Kully's unit

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

got some help from the UK in terms of codebooks which the British had photographed and which Kully's unit was in the process of recovering. There was also another batch of traffic, strain of traffic if you will, that they had discovered in the German diplomatic material which they had identified as one-time pad. Of course as they looked at the messages and tried to examine them there just wasn't enough evidence showing through to get a break into it. Their efforts were further sort of illuminated by the photographing by the FBI of the contents of a trunk or some package or parcel of Dr. Wolfe's luggage when he left San Fransisco without the proper diplomatic credentials and tried to pass through the Panama Canal Zone. Since he didn't have the proper credentials, the FBI took it on themselves to open his luggage and photograph the contents of this box or trunk containing the codebooks, and then after he got his credentials they sort of gave them back and apologized. The violation was already done and there wasn't much the Germans could do about it except fuss. Of course we were delighted because the FBI sent copies of these photographs to Washington. Well when the war started this German effort whil it wasn't destroyed it was certainly diminished because the people with Kully had developed his work on the Floradora were exactly the people he needed when he took responsibility for the Japanese military effort. Kully, I think, was given this because he had more experience in that field than anybody else in the SIS. So it was a good choice. His organization was very good organization.

TOP SECRET
[illegible]

TOP SECRET

I mean it was effective, it was well integrated and well trained. So this was the force in being that assumed the responsibility for the Japanese military and I'm sure that it contributed greatly to the success that they later achieved, and did the groundwork for the training of the new people who were coming in and the techniques which were useful in the solution of the Japanese military materials. In the reorganization, B3 which I was responsible and that's why now I'm telling the story, inherited the Eloradora effort because there seemed no point in cluttering up Kully's unit with this other stuff and since all the diplomatic work been contained in B3 was pretty much of a hodgepodge of systems; the Far Eastern, the South American, you name it. If it was diplomatic we had it in B3, and I was operating under the instructions directly from Carter Clarke which were issued to the Chief of the Army Security Agency, Carter Clarke then being one of the guiding lights in G-2 -- he and Al McCormick of the Chicago newspaper fame were sort of a Romulus and Remus of the G-2. Between them they ran all the intelligence activities in Washington. Clarke's dedication to COMINT, as we use the term today, was exemplified by his order that in our collaboration with the British and I think we should consider this remark as US/EYES ONLY, our collaboration with the British was not only to learn what they were able to do for the immediate purposes of winning the war, but he didn't want to go into the post-war era without having learned from the British

TOP SECRET

every possible thing we could, so his instructions were, "If they' got it - get it. If they know something about codes and ciphers solutions your job is to find out about it and make sure the Americans know fully and we have a totally competent outfit here at the end of the war because we're going to win this war and there is going to be a lot of work to be done in the field of cryptanalysi after the war is over." So under this sort of direction we continued efforts on all the diplomatic stuff and it really paid dividends immediately dividends as well as long-term dividends because we were much better off after the war and AFSA was better off because of these directions of Clark e/. I might observe that the Navy didn't have this attitude about the post-war work because they had turned over all the diplomatic responsibilities for processing to the Army and were concentrating strictly on naval and submarine activities, so it was kind of up to B3 to carry the ~~xxxxx~~ ball for the post-war effort. Now to get back to GEE, ~~there was~~ knowing it was a one-time pad it was hardly any effort trying to exploit the current traffic except to test the one-time pads that had been photographed by the FBI against the current intercept to see if by accident any of these would have been used. But I don't recall any ~~incidence~~ instance of reuse because I think the Germans just gave them up as being compromised and forgot them, never used them. But to satisfy the curiosity of all of us, a small team, ~~of~~ three people, were given the responsibil an of making analytic study of these photographs to see if there wa

TOP SECRET

any evidence of how these pads were generated and put together. And after working quite some time on it, ~~I don't remember~~ I don't remember but whether it was weeks or months, we were well on into the war, it could have been something beyond six months maybe a year and a half, I think the history will tell you that dates exactly. This team discovered certain characteristics of the one-time pads that excited us terrifically. The research was independent and quite without any assistance from anybody outside the small unit of three, ~~and~~ When they found this evidence and presented it to us those of us who had were much more experienced in cryptanalysis than they were, we were shocked into realization that we had something here that might be expanded into a recovery of how these pads were generated, ~~and~~ So we put the best cryptanalysts, the Furners, the Smalls, and the Dan Dribbens, the Walt Freeds, and the John Siemens, and Dale Marston I think was involved in this too, onto a study of these pads with the result that they, in a very short time, figured out how the pads were generated and reconstructed the nature of the machine recovered the machine and the details of the machine which the Germans had used to produce the pads. As a result of this we then in essence could generate every pad that that the Germans had produced you see, ~~whether we captured it or not we had the potential of I mean whether~~ Whether we photographed it or not we had the potential of producing actual one-time pad

keys to be used for German diplomatic stuff. We found out that all we had to do then was to produce the totality of the key in theory of course we had short cuts so we didn't have to do all this, produce the totality of the key and then go through this batch of key which had been reconstructed to find out which particular key was used for the particular intercept that we wanted to read, and this was turned into a pretty straight forward process so that routinely we could identify the key used for a batch of intercepts and exploit in a fairly short time, actually decode the messages we found, worked just as well for current traffic as it did for old traffic. The most dramatic results we obtained from this achievement was to read the messages between the German military mission in Tokyo and the war office in Berlin, because just as we had found in the Japanese Purple and military attache systems, when we intercepted the messages transmitted from Berlin to Tokyo reporting on the findings of the Japanese military experts who had been allowed by the Germans to examine the coastal defenses before the invasion, the Germans asked these Japs or permitted these Japs to go see and went out of their way to show them the strong points of the defenses, and the Japs went back to Berlin and they had experts in air, land and sea and they wrote up a general report with appendices for each, for the land, the the air and for the sea and their estimate of the situation and sent it back by radio because they couldn't get it back any other

TOP SECRET

way of course they wanted to get it back in a hurry. We intercepted it and we were able to read the Purple stuff came out real quick, the MA stuff came out almost as quick because there was a ~~table full time~~ favorable time in our key recovery process, so Ike and Montgomery and Allied Forces in Britain ~~were~~ had this information beforehand and it was ground into their invasion plan and was extremely important obviously ~~to~~ the success of the mission, and I'm sure saved many lives and vital military equipment. Now the this has been dramat this Japanese reporting, but we had exactly the same situation fro Japan because the Germans had been allowed to examine the defense that the Japs were organizing against a possible American invasion in lc the Japanese Islands, ~~and~~ I recall one instance where one of the reports that had been decoded in this GEE system was fed into the armaments group planning group in the Pentagon, ~~and~~ they actually went out to the manufacturer of some of these amphibious landing craft which were being put together for the invasion of the Japanese homeland and modified them so that they would be more efficient in use against the Japanese defenses.

Q: Question ~~was~~ during the WWII was there a recognition of a need lc for a national, that is centralized COMINT effort by the leadershi in ASA (Friedman, Rowlett, Sinkov, Kullback)? ~~Specific question~~ Specific question a.

A: ~~Mean~~ Was this ever discussed among you. Yes but not very formally We sort of assumed that it was vital to have a national centraliz lc COMINT effort in our earlier discussions, ~~and~~ this came in to true perspective only at the end of the war when the problems of what

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

the Army would undertake and what the Navy would undertake had to be resolved in terms of the collaboration between the two and the outcome of it was the discussions, sort of epitomized by the Stone Board and the McNarney ~~McNarty~~ order establishing AFSA. The steps taken along these lines didn't come into being until the problem arose as to how the post-war effort would be carried on. The parameters which surrounded these discussions are basically developed along the lines that each service would have to be responsible for the counterpart intelligence. That was one facet of it. Another facet of it was how best to deal with national cryptography where the same philosophy is employed as we might suggest is employed in this country today where NSA is the master mind in cryptography. Is it more efficient to approach it from a ~~counterpoint~~ counterpart standpoint or from a national standpoint where you have one unit dealing with the army, navy and air, diplomatic or ~~whathaveyou~~ what have you as opposed to the Army dealing with army traffic, the Navy dealing with its counterpart navy traffic, and so on with the air. Now steps taken along these lines were the steps taken to set up the consolidated effort, the Armed Force Security Agency, which later became NSA. The thinking of the Army people I think was conditioned by their experience based on the Army's reponsibility during WWII for the national traffic of the non-biligerents plus the experience we certainly had in terms of the German and the Japanese ~~as~~ because we could see the see the proble

TOP SECRET

EO 3.3b(3)
PL 86-36/50 USC 3605

~~TOP S~~

generated by the counterpart activity namely the Navy's work on ~~Weather~~ weather is the one that rubs me the ~~wrong~~ hardest because there was a lot of unnecessary mishmash going on about responsibilities for ~~Weather~~ weather because the Navy claimed it was essential from the submarine warfare aspect and of course the Army and Air Force, this was before the Air Force was set up separate, had just as a strong a requirement for the same intercept [redacted] ~~and~~ so the counterpart argument then was somewhat weakened because the ~~Weather~~ weather was neither counterpart of the Army or Navy or ~~the~~ Air Force or anybody. It was important to all. So our thinking in the Army was conditioned along the lines that [redacted] and this jibbed with our own experience as we'd observed in our dealings with the broader aspects diplomatic certainly military attache and military air and we were convinced There was no need to argue the point. There ~~is~~ it was, obvious, evident, and all you had to do was to do it, not to break up your effort. Now we also had a certain amount at least personally my great worry was the effort ~~that~~ which we had so worked so hard to build up during the war from the non-~~belligerent~~ belligerent countries of course the Japanese effort, the German effort was completely wiped out for some time after the fall of these two countries, but the

EO 3.3b(3)
EO 3.3b(6)
PL 86-36/50 USC 3605

~~TOP SECRET~~

EO 3.3b(3)
PL 86-36/50 USC 3605

other effort like the [redacted] doing some very effective work on [redacted] we had a good effort on, the Middle East the exotic languages as Cy Gordon called them, the South American countries, we had some very good intelligence from South American messages and then the we also started some work on the [redacted] and other we'd even been intercepting ~~from~~ some Russian ~~and~~ So we despaired at having at examining the prospects of fragmentizing the effort in these areas where the integrated effort was going along so beautifully and to my mind producing efficiently in terms of personnel and resources the information desired. ~~and~~ The counterpart activity was an abhorrent term so far as I was concerned.

Q11

In answer to the question of to whom did ASA report, I think we'd find sort of ~~a~~ the earliest form of one activity being administratively responsible for an activity and another organization being operationally responsible. I use the term administrative and operational here to distinguish between the roles of the ~~Chief Signal Officer~~ who was responsible for the administration of the Signal Intelligence Service and ~~G2~~ G-2 who was responsible for the direction of its intelligence producing activity ~~in~~ less that they generated requirements and indicated priorities. ~~and~~ I don't think this a new problem or a different problem from what we have today except maybe the mechanism today that's used for dealing with the ~~xxxxxxx~~ priorities and requirements is much more complex and sophisticated than it was when we first started out trying to giv

Col Bratton information about the tripartite discussions between Japan, Germany and Italy. Essentially during the war G-2 placed requirements on the ASA cryptanalytic organization which then in turn sent out intercept directives. It was that simple. This was for the Washington operation. In the field a similar pattern was developed where the G-2 representatives tasked the RI companies and the same pattern was followed. It was a logical common sense pattern and its effectiveness and efficiency were a direct function of the understanding of the people who filled the positions at each one of the exchange points in the line of operations. If you had people in G-2 who understood very well the processing problems of the producers, the cryptanalytic group if you will, and if you had people in the cryptanalytic group who understood the intercept collection problems, and if you have intercept collecting people who understood the importance of the cryptanalyst's requirements then you had a smoothly operating mechanism. But if you depended strictly on paper and bureaucratic processes the whole flow became inhibited and snarled up and in many cases required removal of the obstructionist to the empire builders from any of the three points. The way these priorities were expressed so far as the Japanese problem was concerned, and I think this is probably the most important one we had to deal with in Washington headquarters during the war, was that G-2 had a bunch of skilled language people -- intelligence trained, Ambassador Reischauer

was one of the was the head of the Japanese experts who were assigned to ASA at sometime during the war, and I think it was a very effective linkage between the satisfaction of G2 (G-2) requirement and the direction of the exploitation effort, by the translation unit be one and ASA because of Rishires (Reischauer's) understanding of the requirements of G2 and his understanding of what information was available at ASA, and (Then) that was turned into directives to B2 and B3, B2 for the military and B3 for the diplomatic and military attache, which then generated the assignment of intercept facilit: resources to the collection problem. Now any requirements from Marshall or Roosevelt of course would be laid on G2 (G-2) and these obviously would be pretty gross requirements which then would have to be refined by the intelligence experts in G2 (G-2) into process ing exploitation and intercept requirements. I am not aware that there was any requirement that ever showed through being directly placed on ASA by the President. I think this would have been avoided and we would not have known how to respond because we would have certainly wanted to insure that this was being done in the best interest of the country rather than (in) response to a personal wish of the President. Now we did have a lot of that just before Pearl Harbor when the President was directly interested, deeply interested in the messages between Kurusu and Nomura (537) to Tokyo, and in that sense there was a direct

requirement placed, but this was always placed on ONI or G-2, and sometimes through the State Department. DoS

Q: The next question I'll read and instead of answering it I'll comment.

What were the major difficulties encountered within NSA during the war aside from the analysis of codes and the like? Specifically equipment or lack of thereof, obsolescence, personnel or operational conflicts such as the reserve versus the regular army, communications personnel versus intelligence personnel, civilian versus military personnel, army policy of rotation of personnel.

A: I might say in response to equipment or lack thereof it was a dynamic situation. There was never enough equipment. We were behind in our code production problem, the SIGCOM story I think exemplifies the kind of problems we had with cryptography. Fortunately we had the ABA, The contract had been let. the Navy was to receive the first devices. When the Japs hit them at Pearl Harbor the requirements of the Navy suddenly dropped because the battle ships they were going to outfit with the SIGABAs had to be reconditioned and replaced before machines could be issued to them. Conversely the Army was mobilizing divisions like mad and needed equipment. Since we were on the second phase of production this problem was luckily solved by diversion of the equipments in the first phase which were designated for naval activities and provided these equipments to the Army. Actually

the conversion process involved only the change in nameplates because the identical equipments were going to be used in both services, so this was one of the real lucky breaks we had. Now later on there was a requirement for real time communications — particularly between the US and North Africa in terms of mobilizing the US forces and getting them over to North Africa, and we had to have for this on time teletype cryptographic equipment. SIGCOM was produced. It was at first a flat failure because it was unintentionally poorly designed and not adequately tested, but replaced within weeks by the SIGTOT, so it was always a scramble to get something good enough and in quantity enough so that you could satisfy your requirements. Same thing was true of intercept equipment. We always the highest priority for these things, but they had to be built; they had to be shipped; they had to be delivered; and they had to be tested and they had to be installed and all this took time, but it was a normal problem, a wartime problem. I don't think there was anything exceptional about it except that we did as well as we did. Communications personnel versus intelligence personnel - there were some little riffs. Probably the biggest one was the attitude of people who had been trained in Japanese. There seemed to be a little bit of jealousy sometimes between the translators and the G-2 people and the translators and the cryptanalysts, but as soon as this was localized in terms of personalities, the personalities found an undesirable assignment, and I would say it was a pretty harmonious

group. Civilian-military? I've seen captains and majors taking orders from a sergeant or a civilian, and doing it graciously and happy to take the orders because we recognized competence as the prevailing consideration and not rank, and whether you were civilian or military, competence was your badge of authority. Policy of rotation of personnel? If you needed a guy and he had a special skill you put him where he was needed. You didn't do it by the book or by the year, like two years in Washington or two years overseas. If he had battle fatigue you ran him back. If he was fresh and beady eyed and could be used in either theatre you sent him out. You tried to maintain a good balance of capability, Washington versus the field, and here we had some problems of arguing about whether a guy was needed in Washington or Europe but usually we found an answer. I would say these were trivial problems.

A little bit a different aspect of this same problem was exemplified between the attitude of the Army and the Navy ~~versus the~~ in respect to the continuity of personnel. Since the Navy in the days before Pearl Harbor were in the main employing enlisted and officer personnel for the cryptanalytic process, they ran into problems with Navy personnel assignment policy or rotation policy sometimes termed. In the Army when we talked about military personnel, the Bichers, ~~Beechers,~~ the Browns, the Millers, the Cordermans and others, we had exactly the same kind of a problem. But this was a healthy thing in the Army because the continuity, the deep continuity was maintained by Friedman and his group of civilians. So it was a much better thing the way the Army did it with the civilian continuity, at least in my judgment, than the way the Navy did it because we could then

through the rotation of the military--the regular military benefit them and benefit us because we brought the military viewpoint the military requirement, the military understanding directly to bear on the our own philosophy and experience. In the Navy the other side of this was absent because we contributed certain things like depth of continuity and depth of understanding and competence in problems which the Navy lost to some degree because they didnt have somebody sitting on the job all the time who knew about these things from the time they started until the current requirement was expressed. And I think on balance what we did in the Army was a lot more effective than what was done in the Navy.

THE END

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET