

Approved for Release by NSA on  
09-12-2008, FOIA Case # 52318

Oral History Interview

NSA OH-17-82

with

DR. SOLOMON KULLBACK

26 August 1982

Leisure World, Maryland

By R. D. Farley

H. F. Schorreck

*Farley  
H.F.*

FARLEY: Today is 26 August 1982. Our interviewee is Dr. Solomon Kullback. Dr. Kullback is a true pioneer in the cryptologic profession, having begun his career in 1930 with the Signal Intelligence Service at the Munitions Building in Washington, D.C. As a cryptanalyst he was responsible for breaking many Japanese codes, ciphers and machine systems during World War II. Following World War II he served in a variety of responsible positions and, in particular, as Chief of the Research and Development effort. Dr. Kullback retired from the National Security Agency in 1962. Throughout the series of tapes he will recall his experiences. The interview is taking place in Dr. Kullback's residence at Leisure World in Silver Spring, Maryland. Interviewers – Bob Farley and Henry Schorreck. Dr. Kullback desires that this tape and succeeding tapes be classified TOP SECRET COMINT CHANNELS.

FARLEY: I appreciate the time Colonel Kullback, Dr. Kullback, Solomon Kullback, –Kully – that's the name we've heard most of all. What we would like to do is run through your life. Remember the old story "This is Your Life"? To start, I've heard this many times, but just for the record, briefly, before you got into SIS,

your personal background, a little bit of your history in New York, college, and then into SIS.

KULLBACK: I was born in Brooklyn, East New York, 3rd of April 1907. I went to PS 149 which had quite a number of interesting graduates. I went to Boy's High School and then to City College and in City College I majored in mathematics with the idea of teaching in the high schools. I actually did start teaching. I taught in Boy's High, mathematics and then Abe Sinkov turned up one day. He and I had gone to high school together, we went to City College together, so we've been associated for quite a long time now. He came up with an announcement, a Civil Service flyer, for an examination for a mathematician in the U.S. Government. So he wasn't too happy with the high school teaching, neither was I. We were both interested in mathematics more or less using it rather than teaching it to kids who aren't interested in learning anything. So we took the examination, both of us. We passed it and one day out of the clear sky he got a letter from the Signal Corps. I remember it was signed by General Kumpe offering -- No! No! -- The first letter wanted to know what languages we had had. Then after we responded to that letter then a sort of an offer came in, that if we would come down to Washington being offered a junior cryptanalyst at \$2,000 a year -- report so and so. Well, his came second, Rowlett's came first because, Rowlett had had German as his language and then Abe came second, his was French, and then I got mine, the third. I don't know whether it was because of the fact that I indicated Spanish. I had studied Spanish in high school. It wasn't necessarily related to the standing on that mathematician list because I think the three of us were the top three on that list so that it didn't matter. And, of course, Rowlett reported the 1st of April, Abe reported the 10th of April and I reported the 21st of April.

FARLEY: In what year?

KULLBACK: 1930, 52 years ago. Gosh almighty! Of course, first impression, now you say Rowlett seems like a \_\_\_\_\_ picture. In those days he was a much shier or at least more reserved than Abe and I. We had come from a big city, Brooklyn, and that sort of thing and his background in small communities in Virginia. He was much more reticent about indicating anything about when we were talking to one another. Of course, also, I guess one of the first impressions was the emphasis on security. We were told that this was the room, we could work in this room. Beyond this was a vault and there was a line of filing cabinets and if we were ever caught on the other side of that line of filing cabinets, we would be shot, and so on. So that security was one of the very first things. Then Mr. Friedman started us off on a - - we really never had too clear an idea what we were going to do, other than that this allowed cryptography and it was an area in which, you know, you'd be surprised how almost anything you knew would sometimes crop up and be an important something that would be useful. Over a period of time in talking with Mr. Friedman we had told him, you know, we had been studying towards a Ph D in mathematics. He encouraged us to continue, he felt it was very useful and desirable. He got us started off on a program of learning cryptography and cryptanalysis which managed to last for a period of about two years.

FARLEY: Was there a regular training program established, or was it sort of "catch-as-catch-can"?

KULLBACK: No - it wasn't "catch-as-catch-can." Apparently over the years, Mr. Friedman, I think, came in as a temporary employee in 1920, he didn't become a regular employee until 1945. Yes, we had that ceremony in which we gave him the great big medal, as an indication as far as we knew he was the only government employee who was a temporary employee for 25 years. During that period he had several sessions of which they brought in reserve officers and they used to

have these training periods with these reserve officers. So, during that period he had managed really to lay out a program of training. Now I don't know whether he actually had a formal document in which he indicated the sequence in which this training would be carried out, but first thing we did was go through the correspondence courses which were then available in cryptography. Then after that, we got that little red, that book, this (goes to bookshelf, now is showing Mr. Farley the book). The first part had to do with the cryptographic systems. We did a lot of work on that, then this you can see.

FARLEY: That was a regular War Department publication.

KULLBACK: Yes. This was this *Elements of Cryptanalysis*, and this you can see.

SCHORRECK: Was that Parker Hitt?

KULLBACK: No, no, no. This was one that Mr. Friedman had written. Parker had had just a little manual out. I may have a copy written here, but it wasn't very extensive. You can see this is pretty well worn, went through that.

SCHORRECK: You did both cryptography and cryptanalysis?

KULLBACK: Well, we started off first with the cryptography, the courses. The equivalent of, I guess of, current cryptographic courses I and II and all of those things in which you learn different ways of enciphering, coding and went through procedures of enciphering and then coding. Then for the cryptanalysis we started with this – *Elements of Cryptanalysis* and accompanying this was a whole series of problems. When Clark was hired, he came in when we were hired, the three of us and then, let's see, Mrs. Newkirk, I'm trying to remember her maiden name. She was a secretary.

FARLEY: Louise?

KULLBACK: Yes, Louise Newkirk, but that was her married name.

SCHORRECK: Prather?

KULLBACK: No, Prather came later, but it was Louise Newkirk, I believe it was. Then Larry Clark and then later on John Hurt. We had a machine to produce copies, but that was the old gelatin type of machine in which you type the stuff up in the purplish kind of ribbon – ink – and put it on the gelatin.

FARLEY: Hectograph. It used to be called a hectograph.

KULLBACK: I don't remember what it was but this was a machine which would reproduce enough copies of these different problems. Now by actually, let's see, we came in April. I think by 1931, Mr. Friedman was involved in an international conference on communications. He was one of the American representatives and he was to be gone for a good part of the summer and he had recommended that if possible, he'd try to get commissions in the reserves. Now, Abe Sinkov and I had had three years of ROTC training in City College. It was required at the time, compulsory, everybody had to take that. So we then got into the CMTC program essentially while Mr. Friedman was away. We went to CMTC up at Fort Meade for, it used to be a month I think, live in the tents and everything. And that was, what was it, basic, then red, then we were in the white and then the next year we went in the blue and then got our commissions that way. Frank Rowlett didn't cater much to the idea of being away for a month then CMTC camp and so on. Again, one summer around the times, '30 - '31, when Mr. Friedman was gone for several months on one of these international conferences, they had them at that time. It was around that time they finally agreed to the fact that internationally you could now send enciphered material in 5-letter groups. Prior to that, remember the codes used to consist of just sort of either actual words or artificial words because the regulations required they be – sound almost like normal language. Eventually they got down to the point where they agreed that any 5-letter group would be counted as one word for communication purposes and you could join them and send them in groups of

10-letters. These were some of the things which then affected the nature of the communications, the kind of codes that we were constructing and so on. But the point is, when Mr. Friedman was away he was going to be gone for a long time, there was nobody else to conduct the program, you know, that worked for it. The officer in charge of that section, then, was Major Crawford and, of course, he wasn't involved in any of the actual training that we were supposed to get and there were a couple -- two jobs that Mr. Friedman left for us. One, he gave us stacks and stacks of messages which had gone through the War Department message center and we were given the job of compiling frequency distribution. I think it eventually appeared in back of some of the publications and you counted them. About 50,000 letters of telegraphic texts and up to, I think, pentagraphs. So we had big sheets of cross-section papers we'd go through and list 5 letters and move over one, the next 5 letters. The reason I remember that also it happened to be one of the very hot humid summers that we have in Washington and we had no air conditioning in the Munitions Building. All we had was fans blowing and sitting working on the table trying to hold the paper down and sweating. I remember that and gradually we went through an awful lot of drudgery as part of the training which I think was very helpful. Well, first of all, of course, we had no machine equipment to assist us, we didn't get that until about '36 or '37, and so it all had to be done by hand, you know. It was quite a job trying to make a frequency distribution up to pentagraphs up to 50,000 letters of text, believe me. It was good training. I think it was something which the younger generation doesn't get and maybe they don't appreciate what the machines can really do. The other job he left us was an interesting sort of cryptanalytic problem which was to see if we can't come up with some solution for double transposition system. Now he had an approach to the solution of a double transposition system which was a special case, so to speak. If

you had a form that you were using for your double transposition, you know, so many columns, but you're limited to the depth of the columns and you had a very long message, then you would fill in all of the spaces, go through the double transposition and then you would continue with the next part of the message, and then the first part of the message and so on. So, if you had a very long message, but your transposition, let's say, was such that it had a hundred squares, let's say — 10x10 format, then in the end what you really had was a depth of 3 or 4. If you had four hundred letters, you had a depth of 4 in which the same overall transposition had been used in each of the 4 parts of the message. So if you lined them up and then started trying to put together columns you could, in effect, solve that. But that was a special case, what he was interested in was whether or not we could come up with a solution to the case, let's say, where you had just one usage of the form that you were using, so that you had no depths of 3 or 4 that you could line up and try to relate to various columns. That was one problem. We came up with a solution, the fact that it was one of the little black books on a sort of general solution to double transposition system. Curiously enough, while we were going through a period of training with Mr. Friedman in the Signal Corps, Mrs. Friedman in the Coast Guard. She had a small unit in which there were also three people who were brought in. Let's see if I remember their names. Eventually two of them came to ASA, the third one went to law school and set up practice as a lawyer. I can't remember their names. Those two are dead. In any case, it turns out that, again one of these peculiar questions that, the traffic which they were working on in the Coast Guard which was still the Rum-runner traffic because prohibition hadn't been abolished yet and amazingly enough, the Rum-runners had developed a very sophisticated communications system because I think -- well, there were two different groups within the East Coast and one on the West

Coast and eventually, surprisingly enough, retired Navy people had gotten in and had organized the Rum-running fleets just almost like a naval structure with main capital ships, smaller groups and then eventually the littler boats that ran in and out, the speed boats, but they also had a very, for those days, sophisticated communications systems. And one day there seemed to be a change in the nature of the traffic. They were always sending things in 5-letter groups — you know —, this business.

FARLEY: Primarily cipher, was it?

KULLBACK: It had been code. They used codes and there was a change and when you started making frequency distributions, lo and behold, it looked like frequency of English and it turned out that they were using double transposition. The weakness, the way they were using the double transposition, was that in order to maintain the number of letters in multiples of 4, I think they were sending them in 4-letter groups, if the message wasn't a multiple of 4, they added x's at the end and then went through their double transposition. Well, one of the things which helped the solution that we had come up with was that if you could spot these filler letters at the end and know, then at least it gave you a good start — which were the last messages. Actually, all those double transposition messages were solved as part of the procedure. It's again one of those curious things that Mr. Friedman posed a problem, came up with some kind of answer, then shortly thereafter it was actually put to practical use. Now, of course, a double transposition is a reasonably sophisticated idea in cryptography. It gives you some idea of really the sophistication of the communication systems in which these Rum-runners used. Then also, they used <sup>x</sup> extensive code, code system and including some enciphered codes. Now all of this was ultimately grist for our training though, because of his relationship with Mrs. Friedman had access to this traffic.

FARLEY: Did you get traffic from the Coast Guard in volume — for instance all the live traffic — copies of the messages?

KULLBACK: Some of the material that we had was older material. He fed it to us in bits day by day so that we had the equivalent of a day's interception, the day's interception would come in gradually, the volume of traffic built up. We went through the problem of code solution and this was after we had finished the book on *Elementary Cryptanalysis*, which was primarily a cipher system. Then as part of the training for solution of codes we got available some of this Coast Guard intercepted material in which they were essentially one-part codes. It was excellent training in learning how to break into a code system and then towards the end, before prohibition was finally done away with, and all this traffic, there was some live traffic that we got because I think these were new systems and this was ---Well, two reasons: one was to help to see if we could provide any assistance in getting into these things, of course, the other reason is that it was excellent training for us on live material. In the meantime, Mr. Friedman, as I gathered afterwards, for two years sort of had to fight off the Signal Corps people because when we were hired one of their objectives was to start preparing new codes or at least codes. They hadn't any codes really for use of the Army from a division field code on up through codes to be used by the military attaches and then ultimately a new code system for really high level use. And here we'd been hired, three years had gone by and there wasn't, so far as they could tell, any actual useful output. I think Mr. Friedman had his hands full in trying to keep those people off our necks and permitting us really to have the two years of real fine cryptanalytic training that he was able to provide for us, with live material. Everything from simple cipher, plus. Every so often we would get something something that looked like an enciphered message cryptogram that came into the U.S. Government. Eventually it found its way to us because it

had gotten to be known in various areas, FBI, and police and so on that Mr. Friedman was available in the War Department. So it would go to his office and usually he would give us a crack at some of these. It was really a wide variety of things which came our way.

- FARLEY: Did you get any intercept from Mauborgne when he was out on the West Coast?
- KULLBACK: Yes, that came later on. As a matter of fact, he had set up a tape unit, undulator tape unit, (I think it was in his house, in his bedroom) and when he was stationed in Presidio he was copying traffic, Japanese traffic primarily. This would come back and Rowlett would read it and I would write it out.
- SCHORRECK: Had the Coast Guard solved these messages that you were working on prior to the time that you were given them?
- KULLBACK: Yes, they had.
- SCHORRECK: They had already solved them? And you were using them primarily for training?
- KULLBACK: Well, some of them were the very older traffic. I think Mrs. Friedman had worked on and solved them and we got them as training. As our training progressed along then there was a time when we actually worked with the live traffic, the current traffic. You know the systems got more and more complicated and so they were provided jointly and exchanged ideas. So we did ultimately towards the end actually get to work with live traffic also.
- SCHORRECK: What was your impression of Mrs. Friedman? Did you know she was working over there in the Coast Guard?
- KULLBACK: We knew that Mrs. was in the Coast Guard. We met her a number of times because the Friedmans used to, at least once a year, would have us over to their house on Military Road. It wa very charming. We really never got to know too much about the details, knowledge and background but, just between us, really, our impression, and I think it was a mistaken one, was that much of her success was a result of Mr. Friedman's effort. That as the woman, actually the chief

cryptanalyst in the Coast Guard, her successes, we thought, (I don't think that is necessarily so, you asked my opinion from looking in) was that Mr. Friedman really was responsible in working with her on a lot of these problems.

FARLEY: Didn't he spend a couple of weeks with the Coast guard working on a ship?

KULLBACK: At one time, yes, with the Coast Guard working on a ship. So it was our impression, you might say, that the real basic ideas of getting into some of these systems, then she carried it through. But this is not to detract in any way her abilities. She did testify in many many court cases and that a lot of the Rum-runners, bootleggers, ended up in prison as a result of her testimony.

SCHORRECK: Their group did solve systems?

KULLBACK: Oh, yes, they did solve systems. Now the double transposition they recognized it as such, and solved it. Granted it was on a basis of at least ideas that we had written up but nevertheless they recognized the problem and were able to apply the techniques to the solution of actual messages. And also, as I say, towards the end there was one fairly complicated enciphered code system and we were given a chance to work on the live traffic and work with them. So the three guys in the Coast guard achieved successful solutions on what was fairly complicated materials for those days. Of course, one prohibition came and all of that went down the drain and then the three of them were hired and came in to work with us in the Signal Corps. Even Mrs. Friedman stopped working for a while. She then became a consultant for some other government agencies that wanted to establish secure communications systems so she developed secure communications for a number of these new government agencies which had begun to crop up. I think the International Money Fund was one of the things, something like that. But too much of the details of the activities we didn't know because of security, need-to-know, compartmentalization, even though it wasn't described in those terms in those days, was beginning to crop up as a fact.

You didn't pry, you didn't ask questions, do what you were told, that was it. Let me see. Now also in the course of those years. Oh, then, we began after two years or so I think it was, we then began to do more in the way of preparing codes. There were three levels of code systems that they had in mind that we should get involved in. One was division field codes, the other was military attache code, and then the other one was a real high level strategic code for intercommunication by supreme headquarters and so on. It turns out the division field codes we really never used, but nevertheless they were available. If it hadn't been for the fact that the emphasis towards recognizing things became successful they would have had to have been used. The military intelligence code was used and, of course, that was the one about that famous incident involving the military attache in Cairo.

FARLEY: Let me switch sides, please.

TAPE I, SIDE B

SCHORRECK: This is a different one. You mentioned that Clark preceded John Hurt?

KULLBACK: Yes.

SCHORRECK: I thought it was just the opposite.

KULLBACK: The sequence was that Larry Clark came in. He had been working in the District Government, I think, and I think SIS had a vacancy. He didn't come in as a junior cryptanalyst. I think he came in as a cryptographic clerk of some kind and he came and then, of course, in the meantime I guess I'd been looking for somebody with a knowledge of Japanese and eventually John Hurt came to the attention of Mr. Friedman. I mean I don't know what I would have done if we hadn't got John Hurt, but the sequence was Rowlett, Sinkov, Kullback, Clark and then John Hurt - he was the last one hired.

SCHORRECK: Were you working on Yardley's material by this time?

KULLBACK: After we got John Hurt and, oh, I don't remember the exact date, Rowlett seems to have kept records of some kind, because he mentions the dates. John Hurt was <sup>with</sup> us then. He had gone through some of the cryptanalytic training. As a matter of fact, the amazing thing is that famous message about the prison escape in Ohio, Columbus prison in Ohio, which came to us with little <sup>hieroglyphics</sup>. Sinkov, Rowlett and I were more analytical minded, we sat down, we started making frequency distributions. John Hurt never cared about frequency distributions. He couldn't care less, and he was peering over our shoulders and started reading "dearest sweetheart Sarah." And, of course, that's what it was. It was essentially monoalphabet, just the different hieroglyphics with the 26 letters. It was a note from one of the prisoners to his girlfriend. I think he had in there about a proposal for an escape, something like that. That was quite a letdown to us. Here we <sup>had</sup> started off, we wanted to do everything precisely and analytically and we hadn't even gotten through making a full monoalphabetic distribution, and here John was reading it. He taught us something, believe me. We used to have problems with John, particularly once we got into compilation of the codes, and then we started getting galley proofs, you know, to proofread. Mr. Friedman was a stickler that these things must be accurate. you can't afford to have the final things incorrect. Unfortunately, that was a time when John Hurt was still tubercular. He was ill and when he had to do some proofreading, because of his illness he was a little careless about it. Mr. Friedman would try to go through these things and check, so to speak, and find that some errors had been overlooked. It bothered him no end and he bawled us all out and nobody claimed that John Hurt did it. So actually after that, the three of us had our own understanding and agreement. We would proofread everything, even if John Hurt was supposed to, we would take care of that. We

didn't let it get Mr. Friedman upset. John had a perfectly valid reason for that. As a matter of fact, also, there was one year when we went through a reduction-in-force, theoretically, and he was the one who was reduced in force but that was because at that time he was hospitalized. It was a tuberculosis center on Upshur Street. He was the one who was theoretically reduced in force. He recovered and came back again. I mean by that time they had gotten over both the reduction-in-force and the pay. They cut our pay from the tremendous sum of \$2,000 a year to \$1,800.

SCHORRECK: How did you all get along in the group?

KULLBACK: The group – very well, very well.

SCHORRECK: It couldn't have been too many.

KULLBACK: As I say, it was just...

SCHORRECK: Was Sam Snyder there yet?

KULLBACK: No. He didn't come in until about 1936. We were very close. We used to get together socially very often. As a matter of fact, this is an incident – I may have mentioned it about John Hurt. We had a group get-together. It was up at our place that time and there was a box of chocolates somebody had brought and John Hurt went round and asked everybody if you would care for any candy. We thought this was very nice. I mean, after all, he wasn't the host he was one of the guests. Later on somebody went to the box of chocolates to get one and everyone of them had been squashed. The reason he had gone around to ask if everybody wants any was that he wanted to select a hard center. So he squashed them all until he found a hard center. There are more stories about John Hurt really than you can shake a stick at. There is no question that he had a genius of flare for languages. He was always intereted<sup>s</sup> in picking up new words in any language and using the. Unfortunately, sometimes he made a mistake. I mean, I think he learned two words in Russian, one which means "good-bye" and one

which means "thank you" and it got them confused and he met somebody who had Russian background and they were talking and when they were supposed to leave, instead of saying "thank you" or something, John Hurt says "good-bye." The Russian got a little indignant you know and went off in a huff. Well, as it turned out afterwards, when John described it, we could see he'd mixed up the words "good-bye" and the Russian word for "thank you." (Speaks Russian words) These stories really about John Hurt should be recorded because, I mean, his contribution in terms of translating Japanese messages was tremendous, but nevertheless these personal quirks of his character. He had a theory that when you crossed the street, you just ignored traffic rules and you don't worry about cars. You stared at them, just as you would at an animal. Unfortunately one time he was nudged, knocked down by a taxicab and the taxicab man got out, got all upset and runs over to him and says, "Are you hurt?" John gets up and brushes himself off and says, "Yes, John B." and walked off. that should be recorded, really. Then he liked to talk a lot. Also, he had a peculiar habit of eating. We would all go to the cafeteria in the Munitions Building for lunch. John would take whatever items he had selected and arrange them in a semi-circle on his tray and just start at one and take a bit here, then a bit there, then a bit there, go all around. And then he was very talkative, he liked to talk a good deal. One time he opened up a carton of milk, and he's pouring the milk into his glass and then he looks at it and the glass is full of milk all around it. He feels the carton and then as practically all of the milk is still in the carton, and he looks and he looks, and, of course, what had happened, he hadn't turned the glass right side up. The glass was upside down, but he was pouring the milk and hit the bottom and just dripped down over the edge. And to sit across the table and watch this thing. He was a genius so far as the language was concerned, but these peculiar quirks of character.

FARLEY: Absent minded professor type.

KULLBACK: Yes. Of course, also, he had a problem with mathematics. He never got his degree at the University of Virginia. I don't know, it's a shame the University of Virginia couldn't have recognized that they had a genius in linguistics there, but his mathematics was poor because when he (he told us) went to elementary school, when he was in the 5th grade or something like that, when they started dealing with fractions and additions and so on – he had a teacher who was deaf. A woman who was deaf. So when they had to get up and recite the multiplication table, he said he would go through 5 x 1 is 5, 5 x 2 is 10, 5 x 3 is 15, 5 x 4 is 20, 5 x 5 uh hu, 5 x 6 uh hu, as long as the mouth was moving, as far as the teacher was concerned everything was fine.. So that he got out of elementary school, went to high school, went to the University of Virginia, but his knowledge of arithmetic was very, very elemental. And when he had to make change sometimes, he would just hold his hand out and just assume that what he was getting was the right change. It was just a shame, but in terms of languages - - as a matter of fact, he had a roommate who was Japanese. He learned Japanese, and before he was hired, Mr. Friedman had him interviewed. I don't know whether it was military attaches, but some people who've been to Japan had some idea - and they were amazed at his knowledge of Japanese. An individual who had never been to Japan and never formally studied the Japanese language, how well he knew it and spoke it, plus the characters and everything else. You raise the question of Yardley, then about - I don't know when it was - 1934 - I have to look back in the records. One day Mr. Friedman took us down to this vault - the other vault. We were on the third floor of the 5th or 6th wing in the Munitions Building and he took us down to the second floor - one of the wings - and there was a vault door on the corridor which he opened up - we went in. This was a room which had absolutely no windows. The

room which we used to work in, which was in the Munitions Building, had a vault door, but it had windows. It was a regular room except they had put a vault in it. The other side of it was a regular room. (he is showing Mr. Farley and Mr. Schorreck a picture now) That's it, the original. Mr. Friedman impressed on us the security of these things. He opened up the vault - turned the light on - and told us a little bit about the Yardley outfit. These are the files and first thing we had to do was to straighten them out. I remember those grimy films and when we would go down there it was invariably on a day which was hot and muggy and we would all have come in in neat white clothing and go down there and get messed up and everything. These stories have been told. Then actually he extracted from those files, sequences of the messages that were worked on but he just gave the raw intercepts. Then we started working with John Hurt teaching us some of the Japanese. We actually went through and solved quite a number in sequence, so that the material again was part of our training program. But it was the live messages which had been transmitted in those days. The biggest contribution that we would make would be in spotting opened and closed parentheses where they would spell out foreign names and stuff like that which would give an indications. The systems they used were - - the simple systems were ones in which they had two-letter representations for the kana, and then symbols for "open" and "shut" parenthesis, some numbers and standard names and everything. There were some of the Chinese characters, so we could spot the parentheses. They had a ? lithical ? portion so to speak. Begin to guess words and then John would fill in in between the Japanese and so on. And we went through the sequence of systems so that by the time we began to get the live traffic now from General Mauborgne, we had already had exposure to the type of communications which the Japanese were using then. By the time we started getting the Mauborgne traffic the Japanese had begun to complicate

communications a little bit. As I understand it, at least it turns up some subsequent information which became available, that Yardley had been hired by them as a consultant. Of course, after the publication of the *Black Chamber*, I guess, they figured if they were going to make anything, he'd be the ideal man. And they started introducing systems in which apparently they had been told - don't use the same number of letters for each group. You can get more security if you mix up the sizes and so they ran the codes group now with some were 2 letters and some were 4 letters. The 2 letter groups used to be reserved for the more frequent, the basic kana, and then the 4 letter groups they used for the equivalent of the varied Chinese characters and so on. So the first problem everytime they change one of these things and I guess they used to change them fairly regularly. Well, the J series - the J19 which was talked about - that was the 19th of the series as they started using these things. We called the first one J1, J2, so that J19 was the 19th in the series of changes which they had introduced. The first problem was to determine which was the 2 letter groups, which were the 4 letter groups because a 2 letter combination never occurred with a 4 letter group. The 2 letter combinations were always used uniquely and then the 4 letter group was a combination of the remaining 2 letter digraph. In other words, they broke the 676 digraphs up into 2 groupings. One group they reserved for the frequent kana which were then the 2 letter and then the other digraph, they combined into a lot of 4 letter groups so they had a fairly big code to use for the infrequent, like Chinese characters and things like that, so the first problem was to separate the 2 letter groups and 4 letter groups. And this is where we came in handy. This is something that was difficult for John to do. We worked with the live traffic, but again, our really main contribution was because we never really did learn Japanese very well, was to find the groups which were parentheses and things like that. The spelling groups, because we learned

enough of the way in which the Japanese spell things out and what they were talking about to be able to spot those things. It was almost like a monoalphabet and solved those things and John, of course, took care of filling in the rest. For quite a while we would work on these things, but I don't think the material ever went out of our office because there was still sort of a feeling, I guess in the War Department, Signal Corps that this sort of activity was all right if we did in on military stuff, after all part of Signal Corps – part of the Army – but we shouldn't be mixing in with diplomatic traffic, because this is what we were working on was the Japanese diplomatic traffic.

SCHORRECK: Were these drop copies you were getting?

KULLBACK: No, initially, what we were getting was only the stuff that Mauborgne was having on that tape recorder in his place. That was the traffic, but there was enough of it going through that way to Japan that we had quite a volume of traffic to work on.

SCHORRECK: There were no arrangements with the telegram companies at this time?

KULLBACK: No, that didn't come about until much later when apparently military intelligence, G2, apparently got into the picture and there was an approval that this activity was not illegal. For a while, theoretically, what we were doing was illegal because it hadn't been – in fact, with the Federal Communication Commission Regulations, everything militated against what we were trying to do.

SCHORRECK: It was specifically illegal.

KULLBACK: And so, this was sort of kept quiet and Mr. Friedman may have, I guess, the immediate people here, the Signal Corps, may have known that we were able to do these things. We had also been compiling codes at the same time and doing a lot of things, and we were getting some output in terms of the Japanese messages. But you know it wasn't noised about. It was kept fairly quiet. And

then eventually, when they got an opinion from the Attorney General, the fact that this sort of an activity when conducted by the government for these purposes was legal and all that business.

SCHORRECK: Did they get an opinion?

KULLBACK: Yeah, yeah. Before WW II, there was on file in our office, an opinion by the Attorney General that this activity was legal. Could be done. In the file there must be – I know there was this opinion, because my feeling was, well, what the hell, what we were doing prior to that was theoretically illegal. There should be in the files an opinion by the then Attorney General that we could carry on such activities. As a matter of fact, I think this was then also probably the basis by which when we started getting drop copies from the telegraph companies, that this was at least a little security for those people that sending over these things to us was not going to submit them to prosecution by the Federal Government. But there was, I know, that for sure, that there was a written opinion by the Attorney General this could be done. Then you see, by that time, of course, Mauborgne did it because of his interest in cryptanalytic activities. Then where they started – well, then of course – about, what was it? About '32 or so we started getting regular Army officers who came in initially for one year of training, then it was extended at least to two years. So then we had a sequence of Captain Rhodes, then he went off to the Philippines, unfortunately came down with tuberculosis, and so he was retired from the Army. Then Corderman was next and then actually the way it was then set up, Corderman after his two years' training became the training officer for the next one. Let's see, after Corderman, I think we had two — Captain Harrod G. Miller, and the Lieutenant Jones from the Coast Guard. And then after Jones, we got what's his name, Bicher came in, and then an officer who was killed in an airplane crash.

FARLEY: Joe Sherr.

KULLBACK: Sherr. Earle Cook went through, and, of course, I think that's about all.

FARLEY: Schukraft, or did he come later?

KULLBACK: No. Well, Schukraft. I don't think he came in as a student, but he was with us then, because he was with the Second Signal Service Battalion where they started building up the intercept stations. Then we had one at Ft. Washington, and then they put one on the West Coast, Panama, and then Honolulu. That's where I spent a year, '37 - '38, in Honolulu with the intercept group there. Sinkov went to Panama where he set up the intercept. So then by the time this organization was begun to be set up, material was flowing in from all of these things. There was back of this an opinion by the Attorney General supporting it. Mr. Friedman was, I guess, a stickler to be sure that we didn't get involved in anything which all of a sudden pulled the rugs from under our feet. By somebody saying you can't do this and then when we got the opinions from the Attorney General, I think that the government began to realize the way the situation was developing, and that this sort of activity was going to be necessary.

FARLEY: Did you divide your time between compilation of codes and cryptanalysis, or was part of our time devoted to the preparation of codes and the rest to cryptanalysis?

KULLBACK: No, well, you see that when we were preparing the codes, it didn't occupy all of our time. Take a 50,000 word code, which was one we compiled. A famous story I always tell. This was prior to '36, I think it was in '36 that we got our first elaborate machine set up - one punch, one sorter, one reproducer, one tabulator. The way we got that was Mr. Friedman had a friend in the Bureau of Labor Statistics. Bureau of Labor Statistics had a lot of this Holarith equipment. We had worked out a procedure so that if we could use this machine, this was always the goal no matter what we did was mechanized. Even if it was only sliding strips, but something to help in the cryptanalytic procedures and he

arranged so that we could go over to the Bureau of Labor Statistics after their hours in the evenings and use their machines and to compile some of the division field codes. Now, the division field codes were 4 letter code groups of about 10,000 words, relatively small codes. And, Mr. Friedman was able to show the people in the Signal Corps that were using these things, we could compile within a 24-hour period a division field code which doing it by hand with 2x - 3x5 cards would take us maybe 3 or 4 weeks. This impressed them so we got the machines. But, before we got these machines we had actually also compiled a 50,000 word code by getting the permutation table and getting the code groups and getting the code groups on one set of cards and the meanings on another set of cards and neither one be 2-part codes. So we had to scramble either one or the other on this set of cards. And we literally did do that. We locked ourselves in the vault and took handfuls of the cards and just threw them up. Clay(?), he used to claim that some of them stuck to the ceiling. They'd find them. But this was the only way we really could sort them. Friedman sort of had other ideas for example, one time he had a picture of putting the code words on slugs like your printing slugs and mixing them up, but with 50,000 -- . So then for example, once, we had accomplished this, and then we had merged. So we now had a code group and the meaning with let's say in the code groups in the mixed up order and the meaning in alphabetical order and had it packed up and then re-phabetized so that the meanings, the code groups, were now in alphabetical order and the meanings or whatever order. Then sent this as a manuscript to the Government Printing Office -- it had to go to the Government Printing Office. Now there was a means whereby, as far as I know, the Government Printing Office had vaults and secure places, and these things were presumably worked on by a limited number of people, because what would be the use of having these high strategic codes if they were just available to anybody in the

Government Printing Office. Now, of course, one this went over there, it took a long time for them to set the type up and give us the galleys. We would get the galley, so that when we were working on a code it didn't keep us busy every day, so we had plenty of time in between to do some of this cryptanalytic work that we were working on. So it was a matter of fitting in to the spaces, plus the training. You see, we were assisting in the training by then. We now had these officers and we took care of a good deal of their training, giving them the problems or lecturing to them. So that it was always something going on.

FARLEY: Did you compile the War Department telegraphic code? The one about the Sears and Roebuck Catalog size? Remember that was 5 letters.

KULLBACK: No.

FARLEY: Was that WW I?

KULLBACK: That was really used only for commencing the traffic. It wasn't considered secured. The one we compiled was never used, actually was never used. In fact, the only one of the codes that we compiled that was ever used was this one for the Military Attache that Colonel Keller in Cairo, because in the meantime, the effort was towards mechanizing. And, of course, what's his name, Parker Hitt, when he retired, he went to work for the IT&T, and then he came and offered his teletype automatic to the State Department. Again, Mr. Friedman was very friendly with Sammon, who was running the State Department communications. Sammon came to us to advise him on the security of the device, and so we worked on the IT&T machine. Then, actually, you know, the Germans then adopted and modified it. Because the weakness of Parker Hitt's machine was the fact that the wheels he used to give off-and-on impulses was fixed. I guess it was a big wheel with little notches cut out of it. It was fixed, you couldn't change anything. What the Germans did in their Geheimschreiber was replaced those, I guess, by push button that you could set off and on, so you could vary the

*PARKER  
KELLER'S  
M.A.S.*

activity, just like in the Haglin. You could vary the activity. I guess essentially that was the biggest difference between the IT&T machine and the machine that became the German Geheimschreiber. Scrutiny there was the fact that you could vary the buttons, but I think, of course, it was also 10 wheels and 2 wheels interacting to produce a series of off-on signals which would encipher the 5 positions of the teletype code. They took the IT&T machine. I think that it had been offered to them and they saw, too, that to get security you needed flexibility in being able to change it, 'cause actually, when we got the series of test messages in, I don't think it took us very long to solve them. Also, it had another particular weakness. It was presumably operating on line so that the operator could -- the teletype circuit could be operating in the clear and then he could cut his machine in and then when he finished his encipher transmission, he had to punch 6 characters which, in effect, cut the machine off and put the teletype line back in the clear. Well, all we did was look at the last 6 characters in the transmission and we had sliding strips, we had put these wheels on -- we bought rulers with -- with cross-section paper, we pasted the stuff down and that was our mechanical device and sliding them back and forth, it didn't take us very long to solve those ITT.

FARLEY: Let me switch cassettes, please.

TAPE II

KULLBACK: It's rather, as I think about it, a shame, but I guess the nature of the activities was such that we really couldn't advise Parker Hitt (the IT&T people really) about what was really the weakness of their machine. In other words, the machine was submitted to the government for possible use as a secure device. We solved the messages. They gave us a series of test messages and we read the messages and

gave them back to them. But, I guess there was no way really in which we could have made some suggestions as to security. I mean, it was unfortunate. At that time, mostly, the development of secure communications was up at Ft. Monmouth by the Signal Corps, and again, unfortunately, they may have been good communicating people, the engineers, but, I think some of their notions about cryptographic security were not too good. It conceivably could have been followed up. I mean the way the Germans did and got a Geheimschreiber, and, of course, the Geheimschreiber was also read, but it was a little bit much more sophisticated job to read the German Geheimschreiber with the Collosus and all the other machines that were built to do the reading. Then, again, during that period of time, whenever Mr. Friedman got notice or came across any information at all that there were cryptographic cipher devices that might be available, eventually he managed to get the Signal Corps to buy at least one copy. So we had the Kryha machine.

SCHORRECK: Enigma?

KULLBACK: No, no, first the Kryha. We had the Kryha. That was a device with two, one fixed vane(sp) and then one which used to rotate. And then you could rearrange the little segment to change the alphabet, but the wheels which controlled the motion were fixed. It was a wheel which had holes punched in it like a clock but at different intervals, so it would rotate on this spring wound thing. The thing would rotate until it went from one hole to the next hole. So sometimes it would move two spaces, sometimes four spaces, but that was a fixed cycle of seventeen holes on the wheel. That wasn't very difficult, I think we were able to write up a general solution. Now another thing at that time, once we started working on it, Mr. Friedman was rather insistent that we start compiling technical literature, build up technical literature. Whenever we worked on any of these things we then wrote up the solution to these things. Whenever funds

were available, particularly toward the end of the fiscal year they had money left over, then he was able to go to the Government Printing Office and have them print up these things. That's how that black book series came about; only because money was available at the end of fiscal years. I shouldn't say it I guess, but one never turned back money to the government. You always found some way of using up whatever money was left at the end of the fiscal year. So the Signal Corps would come to him and say, "We've got a couple of thousands of dollars. Do you have anything that we could use up 'til June the 30th?" He'd go to Government Printing Office and give them manuscripts. So these had all been compiled. There were two things really that he kept on stressing all the time. One was, you write up these things in the proper technical fashion. He was always insistent that we must use reasonable technical terms. He didn't like fancy words, but it should be a technical literature with a technical language. Of course, the other thing was always mechanize. See what you can do to convert these hand operations, the procedures which can be mechanized to speed things up. So, the Kryha came along, and we solved it. Now that had been brought and we solved it for our own amazement or amusement, so to speak. And then there was another machine which came into being which was a Swedish machine. Well, I guess Damm was the inventor, but this was one actually which the Russians used for a while. Now we didn't know that. We'd gotten the machine which involved first, a substitution of the letters in the equivalent of a square. You had the coordinates then the coordinates separately were enciphered through rotors and then the thing was recombined. Then we wrote up a solution. We solved such a machine and we wrote up a solution for that. Then it turned out later on that this machine had also been bought by the Russians and they were actually using it for a while until they started building their own devices. Then, in the meantime also...what's his name...five rotor machine...?

FARLEY: Not Hagelin?

KULLBACK: Not Hagelin...

SCHORRECK: Hebern?

KULLBACK: Hebern, Hebern, Hebern. He was working with the Navy, and he had gotten them interested in that original five-rotor machine which Mr. Friedman had solved before we ever came in. This was about '27 - '28 -- that order of time. So the Navy, of course, dropped any further investigating of that machine, but Hebern continued working, I guess, in conjunction with OP-20-G at that time. Then another problem which is next in sequence in which he made certain changes in the order of which wheels moved and so on as the result of Mr. Friedman's solution. Then the Navy, even though there wasn't, really, too much cooperation between the Army unit and the Navy unit in those days on the surface, there was this. Mr. Friedman had good cordial relations with some of the Navy people, so there was an interchange of, not necessarily ideas, but, for example, when they had the Hagelin machine, they would use us, let's say, as a means of seeing whether it could be broken into. We had an understanding. They would give us so much traffic, and we had some ideas about the machine. In other words, what an enemy might be expected to do. You know, real security studies. That's the one which is also written up in one of the black books; the solution of the next version of the Hebern machine. We finally solved that. It took a tremendous amount of experience. We wrote it up. Then we also had another challenge. A modified Kryha. That's the one Callimahos, I think, wrote up. What Kryha people did was, instead of having the mechanism which moved the rotors fixed with the opening, they made it so that you could, with little pins or something, change the openings on the mechanism which drove the rotors so that you could change it from message to message. It wouldn't necessarily be the same motion, which was the original weakness, and they

wrote these tremendous blurbs about the security and millions and millions of possibilities. Eventually we had this challenge and they were told, well, you submit a certain number of messages and so on and that sort of thing. Callimahos wrote it up. The messages came in, Mr. Friedman time-stamped it and we worked on it and then we took a break for lunch, and then we time-stamped it again. It took about a total of two hours to go through and solve the series of messages. So that was another one. But again in the meantime the Signal Corps had devices which they were submitting. Eventually I guess maybe they came to realize, and I think whatever little money there was available for development of such devices was turned over to the field office in Washington. The responsibility for the development was given to Mr. Friedman, the signal intelligence rather than another element because Ft. Monmouth had come up with a device which was really out of this world. In order to mechanize they had a weight which ran a cord which ran over a pulley into the machine that was supposed to provide the equivalent of a spring motion or something like that. And the security wasn't particularly good. I mean, it was really a waste of time and money for those people who had worked on it. Then along came the Hagelin Two. We worked on that device. I think those were all the devices...oh, the Enigma. We also had an Enigma, what we had, though, was a commercial Enigma, not the German version. We had a commercial Enigma and on that, too, we had messages which we had solved and were able to reconstruct the wiring and do all of that thing. And so we had as part of our training, or at least exposed to a wide variety of devices which were being built, and compiling the codes in the meantime. Then along about '36, this was, the Japanese introduced a new system, which we called then the Red Machine. This was a machine, the first machine that they used. I know it was '36, because that picture was taken in 1936 when Sinkov was going to go to Panama and we had been working on

those messages before he was destined to leave to go to Panama and we finally got the complete solution while he was in Panama. So I know it was about 1936. Eventually it turned out that that machine resembled a machine which the Japanese naval attache was using, and the Navy people had solved it. They just wouldn't give us the details of that naval machine. As I understand it their argument was essentially, the Navy unit, you see, was exclusively Navy people. They felt that the security was much better than the Army group which were civilians. You had no control over civilians so to speak, whereas Navy people were subject to court martial and so on. What I personally find rather amusing in all of this is that when you read all these books which have been coming out -- *AT DAWN WE SLEPT*, and *ULTRA* and *TOP SECRET ULTRA*, there are more interviews with Navy people than ever there were interviews with Army people who spilled as much of the beans as the Navy people were spilling. Maybe by that time it wasn't so secure, but these books contain a lot more information from interviews with the Navy people than ever they got from the Army! But that's beside the point. There's no question the coordination between the Navy and the Army, in this business I guess as well as others could have been a lot better. I think partly that business about Pearl Harbor was possibly a lack of coordination, but actually, as I read their ideas about what happened to Pearl Harbor, I think, well -- in any case, let's get back. Again, it turned out that this machine was very, very much similar to Kryha tack device. What the Japanese had done, was again, they divided the alphabet into, initially, 6 letters, which were supposed to be the 6 vowels and then 20 which were the consonants, so they had two wheels, one wheel of 20 and one wheel of 6 which were geared together and for each key that you pushed, they would rotate simultaneously. And if it was a vowel, because of the nature of the kana, which is essentially consonant, vowel, consonant, vowel, they wanted it to resemble their old

systems externally, and so they would encipher vowels by vowels and consonants by consonants. And then because of the nature of the language when you looked at it it seemed to run consonant, vowel, this sort of thing. So it didn't look like a machine or anything else. They had a mechanism with variable spaces which would then rotate these things. And then you had a fairly long cycle, so if you got very long messages you could find repeats at intervals and look like tremendously big polyalphabetic message which is presumably what it was. But we did get, or at least Mr. Friedman did get a hint from some of the Navy people that he was very friendly with. He maintained good relations with some of those people and it helped in, you know, figuring out. And so we had a complete solution for that Red machine. It wasn't very difficult really for us to work out which were the 6 letters and which were the 20 letters and determine the motion to solve those things. This was a good deal of the traffic we were beginning to get from Mauborgne also. By that time we also had the set-up in Honolulu. When I went to Honolulu in '37, one of the things my assignment there, was to select all of these Red machine messages and encipher them and transmit them back to Washington. The Chief Signal Officer out there in Honolulu, I think he used to deliver them. He had an understanding where I gave him batches of messages which were in code and they would be transmitted to the circuits back to Washington – no questions asked. I think he had some idea of what it was, but you know, this was – so I used to get the intercepts of the station. I was in one dugout overlooking the harbor there in Diamond Head – it was beautiful. There used to be the old Coast Guard gun emplacements which they had taken out. I mean they weren't useful anymore and they had built windows across the front of it and gates and so on, so it was a secure area. You couldn't get into it. One dugout here was where the intercept station was and I was next door, and I would get all the intercepts and go

through them and pick out those that were Red messages I could recognize. Then we had set up an enciphering system which used the strips – the 26 strips and I would encipher each, start you know with the ordering of the strips and then – let's see – start and go down – the sequence in order 1, 2 and then keep on going around, and changing it for every way you start a message. At the other end Rowlett would get them and he would decipher them. Sinkov was in Panama at the time. I guess most of this traffic was coming through Honolulu on the way to the Far East. And in the year that I was in Honolulu there was a tremendous volume of traffic. There was never a single mistake – never a single mistake – that was something Frank, I think, mentioned also. He would decipher the messages – never any problems about garbles or anything. It was really, well I can't say it was really my fault, after all, we were trained just for that sort of thing. I would go solve some of those messages, but my knowledge of Japanese was not enough so that I could really give a good translation of these things. If we'd had a translator along with me we could have been reading all those messages out there, but, of course, they were read in Washington. That was then the Red. Then, of course, the Purple came along much later. This business about Pearl Harbor – I think what had happened was the Signal Corps, the intelligence people – this is my own idea, may not be worth a damn – but, the cryptanalytic skills that we developed and our capabilities, at least in reading the Japanese material, really went beyond possibly either the appreciation or the expectation of the military intelligence people. They had a wonderful force here, a wonderful tool, but they didn't know how to use it. They had no idea about setting up the system which was set up later on with security officers who would get the material, make it available to the commanders and then make sure security was followed and things were done. And, of course, they were so concerned about maintaining the security of the source, "Magic" so to speak,

that maybe the tremendous limitation which they imposed on the distribution and I guess the evaluation and interpretation of the material just didn't keep up with the volume of material which was coming through. So that a lot of cracks in the system, unfortunately I think came through. Now, of course, so far as the business about Pearl Harbor is concerned I don't know, but what in the end and in the long run, even if it was a deliberate attempt to have the Japanese attack and not know that their stuff was being read. In the long run, I guess, the sacrifice of those who were killed at Pearl Harbor saved a hell of a lot of others who might have been killed in the results afterwards. It's hard to say, but I think partly that the problem was they had developed a tool a lot maybe faster than they developed the ability to exploit the use of that tool – the cryptanalytics and the way the messages were coming in. I don't know what went on in G-2, but as you read now about the history people who delved into what was going on and so on, this is the impression you get. They didn't set up an evaluation center – a real place where these things funneled in. They could interpret, appreciate, analyze, do what was really necessary to exploit the tool and then, of course, they were so jittery about keeping it all secret. Maybe, as you read that book, especially the communications back and forth between Washington and Pearl Harbor what went on, then you can begin to sense that. Well, let's see what else.

FARLEY: What are we up to – about 1937?

KULLBACK: This is '36 - '37.

SCHORRECK: Did you go to Hawaii to set up the intercept people there or to just do those messages? Or both?

KULLBACK: Well, no, the intercept station was already going there. I was sent to Hawaii to a certain extent primarily to be able to pick out the Red machine intercepts, encipher them and pass them back, but also to train the intercept people in cryptography and so on and, but we never had enough people to try to do what

the Navy had done. Now, for example, all the time that I was in Hawaii, at the same time as I find out now, the Navy had quite a cryptanalytic outfit which was working on the Jap Navy messages. Now I didn't know the existence of such a thing.

SCHORRECK: And they didn't know about you?

KULLBACK: Well, I don't know whether they knew about my existence, but we never communicated. I never communicated with them, see.

SCHORRECK: We see very little about the unit at Ft. Shafter. Do you know why that is?

KULLBACK: That unit at Ft. Shafter?

SCHORRECK: The Army unit at Ft. Shafter.

KULLBACK: Well, this was what I'm talking about – theoretically, I worked out of Ft. Shafter.

SCHORRECK: We've seen very little of it – even anybody that was there.

FARLEY: Was there a unit designator at all? What was it called?

KULLBACK: It was the intercept station, that's all. What they did gradually before the war, the outfit – the intercept station, which was in the old bunker in Diamond Head next to me, they built an underground chamber, bomb proof and everything. After I left, out someplace in one of the pineapple fields, as I understand it, and after I left in 1938 to come back, ultimately they moved the intercept station from Diamond Head to this underground bunker. That was – this was essentially the Ft. Shafter outfit. I worked out of Ft. Shafter, I reported to the Chief Signal Officer, Colonel Sandtler, I think it was, whose office was in Ft. Shafter. I would take the day's output, the messages which had accumulated, which had been enciphered, and would drive out to Ft. Shafter and turn them over to him and they would be transmitted back to Washington.

SCHORRECK: Wasn't any processing done there?

KULLBACK: I did all the processing.

SCHORRECK: How about when you left? Did they have that capability?

KULLBACK: No. When I left, that stopped.

SCHORRECK: They just sent stuff back?

KULLBACK: That's right, they just sent the stuff back.

SCHORRECK: What was the difference between your outfit in Ft. Shafter and the one in the Administration Building in Pearl Harbor - - the Navy. They had a huge processing outfit.

KULLBACK: The Navy, as I find out now, had a complete intercept, translators and cryptanalytic, and they were working on the naval stuff. Now, of course, there was also a big difference between - see we had access only really to the Japanese diplomatic stuff, because we could pick that up at the intercept station. We had no really Japanese Army traffic until they started spreading out into the Philippines and there was close contact and we could start picking up the material. When they were in China, when the Japanese were in China, going all over China, we had no intercept except maybe an occasional message. We would see which the (U.S.) Navy ships, you see the Navy had ships out in the Far East - they were picking up what they were primarily interested in was Japanese Navy traffic. So the Navy had intercept facilities on some of the larger vessels long before the idea came up about outfitting these ships which would do these spy ships so to speak, and occasionally they could pick up some of the Japanese Army traffic. But we never had any reasonable volume of traffic to consider working on until the war started and then of course when the Japanese moved out of China and came down into the Philippines and Malayasia and all of that area, we started getting the volume of "2, 4, 6, 8" that was the first one we got any great volume on and it was worked on both in Washington and the outfit in Central Bureau.

SCHORRECK: You didn't have any degree of control over the intercept development in any way, did you? In Arlington Hall - I mean at the Munitions Building?

That seems to be a separate thing under the Signal Corps.

KULLBACK: Well, there was a coordination, eventually, by the time it was built up by Schukraft who had something to do with it in Washington. I think it was built through Ft. Monmouth and then they established a Second Signal Service battalion, but I think the decision as to where to put the stations was probably coordinated with our activities. But where did they go? They went -- first of all we had military divisions. We had one in Honolulu back in '37 when I was there. In fact, it had been set up before I got there. There's one in Honolulu, there was one in Panama, because when Sinkov went down there --

SCHORRECK: Didn't we have one in Ft. Wood?

KULLBACK: I don't recall one in Ft. Wood -- the, of course, there was one around Monmouth, and then there was one put in in the Washington area at Ft. Washington, I think -- and then San Francisco. They put one in in San Francisco, and eventually got one in the Philippines. That went on primarily through, as I remember through, Ft. Monmouth. It was that was strictly all military and no civilians. It was all the soldiers, their training, I guess their equipment, all was handled by the Signal Corps through Ft. Monmouth. I guess the decision as to where they would go and so on then eventually they were all tied in with the Second Signal and then the, I think by that time at least the liaison was maintained with out office. Schukraft, for example, had a good deal to do where there was intercept outfits. Then as we started getting graduates -- for example, Corderman took over from Rhodes<sup>AD</sup> in the Philippines. While I was in Honolulu, Corderman was in the Philippines and on his way back he -- went down to the ship and met him and ships were allowed layover a day or so, in Honolulu. Essentially he was a replacement for Rhodes<sup>AD</sup>, because Rhodes<sup>AD</sup> got sick. Then as we got more of the graduates, we got more stations, then I think we began to put in these Signal Officers, but primarily as Signal Officers with a background in the various

stations, so it began to build up. And at least that's why I say, this sort of activity was well prepared, you might say, for '41 when things finally happened, because we had the intercept stations. At least in the position to receive traffic. The diplomatic traffic on a commercial channel was no problem, we could get those, and as soon as the Japanese moved down to where they were in range, because initially you know, they would keep the range of their transmissions down and they were security conscientious too, so we couldn't get anything. But once they had gotten into the Philippines and so on, then we began to get a flood of material and so the break was made into the 2-4-6-8. A lot of people don't understand this and they wonder sometimes why the Navy was working with JN-25 before, they were doing the work on the Jap Navy and the Army apparently didn't know anything about anything. I mean, you get the implication. I mean, the Navy was doing it and when you read about it, there is nothing about any of the Army. All you hear about maybe is the diplomatic traffic, you see. The actual fact of the situation is we didn't have any traffic to work on.

SCHORRECK: I understand that even after we did get to Japanese military some of it was very hard to get into, too.

KULLBACK: Ultimately, we got into every bit of traffic. Well, as I say, '43, April, we got into the 2-4-6-8 and then thereafter, we were at the administration system, the air system. They even had a special code that they were using for radio communications and there wasn't a damn thing that the Japanese transmitted that we weren't able to read, and if that stuff was ever kept, there was still tremendous amounts of messages - more than the translators could go through and really more than the intelligence people needed to maintain the battle order and everything that they were really looking for and interested in. Again, you see confusion is between the Enigma and in the kind of communications the Japanese used. In the Enigma, once you got in one message in the key for a

particular unit distribution, I guess they used different keys for different kinds of organizations, but once you read really the first message, you could read all of them because it provided you with the clue to the setting. So you set your machine, then you could read the message. Whereas, in the code system, in the first place, an enciphered code system, first you had to reconstruct the code, and secondly you had to recover the keys. If you got traffic on a page in an enciphered system which hadn't had much traffic usage - you didn't have the key - - you couldn't read those until you accumulated a reasonable amount of traffic so that you could start reading those things. Now, the Japanese used a 10,000 word code book; of course, they were 4 digits and they used all the digits. They also used, you remember, 500 page key books - had 500 pages with a square on it 10 x 10 with coordinates row and column in a random order and then instead of using normal arithmetic to encipher the messages, they actually used a 10 x 10 square so that T-5 and a plain number 2 didn't add up to 7, it would be 8 or 9 or something else. They also used a separate system for the addresses - the addresses had their own code book, their own key book, and their own squares, so that if you were really going to get in and get a good idea of the traffic - - who it was going to and what it was saying and so on - - you had to solve the address system. You had to solve the body of the system itself, and you had to have at least a reasonable number of messages using the same page of the enciphering tables. Now, of course, when we started getting a large volume of traffic those conditions began to be met and so in the end, because at least we in Washington in the B-2 section - our philosophy is we didn't give a damn what it was - - were going to learn everything we could about the Japanese Army systems. And if anything was captured, anything was found, we knew enough about their usage so that we could take advantage of any of the captured material. If we had done what originally the translators wanted done -

- once we got into 2-4-6-8, the translators were - - they didn't care about anything else. This was ideal, turning out messages and we were sinking the Japanese ships and so far as they were concerned - - forget about everything else. Of course, as a cryptanalyst we wouldn't do that and so we then started on the administrative systems.

#### TAPE TWO, SIDE B

KULLBACK: For example, the high level systems, they didn't want to pay any attention to 2-4-6-8, because the high level systems gave them a hell of a lot more information than just information about the movement of the ships, and then the same is true with the Air Force system. So, we were able, and we got into reading all of these and, of course, if anything was captured, our knowledge of it was such, even if it was like the communications systems. We knew enough about them so that when we did get some messages - - maybe we didn't have enough messages to be able to do much with it, but if they captured a code book or a key book for one of these things, well, lo and behold, we knew enough about it so that we could relate the captured material to whatever intercepts we had. So, everything we had in the way of Jap Army materials which came at least into Washington, everything was read, was decoded, was available for translation and for interpretation, as I say. There was such a volume of material, such a volume of material that it really wasn't of interest to the translators and to intelligence people because they were getting enough of what they needed and they were primarily interested, of course, in reconstructing battle order and knowing where the Japanese and the messages about the casualties. You know the Japanese had a very funny system of operation. Each unit was tied in to its home base in Japan and no matter where it was stationed, that communication

would go back to a home base in Japan. So when they were reporting on their casualties it would always go back to the home base in Japan, so we, at least the intelligence people, had a pretty good idea of the casualties, the strength of the units. When they needed reinforcements it would go back to the - - it was a very funny system, however. Very much different from the way the Americans operated. I mean, granted a division may have had a home base, but once it was in the field, it operated within the Corps or within the Army. It didn't go always back. Another thing, I don't know how much the volume is known. For one thing, we kept in our B-2 section, Bill Erskine, Hugh Erskine's brother, he was the center into which we focused or sent all of the serial numbers for every Japanese unit which was transmitting messages, so that when the girls were working on the depths which start and want to know entry clues, we could tell them. If we knew the unit, go back, that the last message this unit had sent on such and such a date was number 352, they would number them, so you could get an idea that this might be 353, 354 with which was good break into the system. Also, there should be in the file some place, this was after the war, when we were looking for things to do to keep busy before we reorganized and everything. We asked ourselves a question, which in effect, was; here the Japanese who developed really quite a sophisticated communications system encoding and enciphering, sometimes we wondered how the Japanese were able actually to communicate with the amount of pencil and paper work that was necessary for their systems, with a separate address code book, separate key book, and an administrative code book and key book. When I used to give lectures to visiting people about it I used to take them into a room, and had a table piled high with materials, and say these are the current materials which are being used by the Japanese in their communications, an awful lot of handwork. What caused not only the loss of the war, but actually they didn't have any cryptographic security really is what it

amounted to. And Bill Erskine wrote up quite an interesting analysis of their security, their penalty, you know, during the war there were a lot of some captured materials - some of the Japanese ships that were burned and sunk, divers went down. We got pretty charred books which came back through Central Bureau, eventually, I guess, it came to Washington. And Colonel McGrail in his chemical laboratory, reconstructed it. Really amazing, you know, they were able to bring out from the charred material the numbers which were printed there. We had photographs taken and in a number of instances we actually were reading the messages with the captured material in which the Japanese sergeant, or whoever was in charge, described in considerable detail where he had dug a hole, how deep the hole was, how big a fire he had made, how he had burned this particular book in which we had our possession, how he had stirred the ashes, dumped them into the hole and covered them with sand. Now, one of the reasons for that was, the Japanese had imposed penalties and if anybody in the chain of command, if the private or the sergeant or the corporal who was responsible for carrying these books and so on admitted to the loss of these things, he would be punished, his supervisor would be punished, right up, I don't know how high up the line they would go. Consequently, there was every reason under the sun, so far as the Japanese were concerned, not to admit the loss of any, or the capture of any, material. So there were many instances in which material was lost or captured. They didn't have time to burn it up. The scheme was they would tear off the covers and ship the cover back as proof, you know, that material had been destroyed in accordance with orders. Now whether they had a more reasonable system which wouldn't in effect penalize everybody in the chain of command so severely, there wouldn't have made that much difference in I guess the crypto. Once we had gotten in they couldn't shake us loose. This is one of the things - - they made their penalties so severe,

that in effect the people ignored them. I mean, they were afraid, a sergeant would be crazy, really, to admit that he had lost a copy of the book. The penalties were such that he and his lieutenant and his captain would all get punishment, so why admit it when you could write up a fancy story. Then, of course, there were also certain instances where some of these ships went down, material was destroyed and we never recovered it. They assumed that it had been captured and they would make changes. I mean, so it works both ways. But, that document of his sort of - the analysis of it - the whole Japanese procedure - their security system - their philosophy is a very interesting document. I don't think it has ever gotten the publication and distribution within NSA which I think it merits.

SCHORRECK: I don't know if they could find it.

KULLBACK: Well, I don't know, they should find it provided I --

SCHORRECK: You overestimate the files.

KULLBACK: Well, I don't know. Well, they file these things someplace in Kentucky, I guess it was - went to a central location.

SCHORRECK: They're back from there - they went over to Holabird.

FARLEY: Did they go to Crane, too?

SCHORRECK: No, they well - some of them did, but they are back from Crane.

KULLBACK: Well, I don't know, if that thing could ever be found, I think it'd be worth, as a document, let's say, even for the crypto-school, for the people who are coming up. Here was our evaluation of what the Japanese system was and the weaknesses. Yet, you see, the Japanese, in theory was quite a sophisticated system. They really broke down the contents of the messages into several parts, the address, the radio call signs had their own schemes, the address was altogether different, the text itself, plus the encipherment table, plus the fact that they didn't use normal arithmetic. Now in the 2-4-6-8, they started out with

normal arithmetic initially, then they introduced the little squares, which initially use on the indicators which gave the roll - the page and the row and column for the keyboard. And I thought that was, in theory, a reasonably sophisticated system. Actually, the codes that we had prepared, our military intelligence code that we compiled and that Colonel Feller<sup>s</sup> had were similar to that except we didn't use number code groups, we used literal code groups and what Colonel Feller<sup>f</sup> had was a series of alphabets to encipher the code groups with key systems and so on. We assumed that that was a secure system. When it came to our attention in 1942 that the Germans or the Italians were reading his traffic, we just couldn't believe that it was done purely as a cryptographic solution. Of course, as it turns out, subsequently as was found out, that this wasn't done purely by cryptanalysis. The Italians apparently had intercepted and copied - - had gotten the bag in which his code book was being sent. So they got a copy of the code book and they also were able to get a copy of his enciphering table. So that if you had all of these things it wasn't so difficult as a cryptanalytic problem, there wasn't such a difficult problem. But I say initially when it was called to my attention, I was in England at the time, at GCHQ, and they were reading the Geheimschreiber. There were indications in there about the Germans reading Colonel Feller<sup>s</sup> material and sending the information back to Germany. The British called me in and called my attention to it, so at least I could convince Washington some changes had to be made. I just really couldn't believe it because I said I worked on the compilation of that code book. It was a two-part code and the enciphering system just didn't seem that it could have been a purely cryptanalytic effort.

SCHORRECK: Didn't you have some trouble convincing Mr. Friedman?

KULLBACK: No, no, I mean once they saw the, or at least the fact that the Germans were reading it. I gave them the message number, then they could go back and

compare the messages. The next thing that they did was to send Colonel Hiser out to Cairo with SIGABA. Then after that, all of this stopped. No, there's no difficulty - I'll tell you, there's one thing. Mr. Friedman never took the attitude that apparently both the Germans and the Japanese military as you find out now, there are all sorts of claims made that the Japanese had been told that the Americans were reading their communications so they made checks and they were convinced there was nothing to it and they kept on using the Purple system. The Germans again, both the Germans and the Japanese were more physical security conscious than they were really cryptographic security conscious and with Mr. Friedman there was no such division. He was cryptographic security conscious, and I mean physical security conscious also, so that when this information turned up like a light in the German traffic, there was no hesitation in the traffic, no question about it, Hiser was on his way with a SIGABA to Cairo in a very short time. Without saying, "Well, look, we compiled these codes, two-part codes, we know the cryptographic system, that was a good system." There was none of that bull. Whereas the Germans and the Japanese, at least the people responsible for these things were more inclined to feel, "Well, look, we compiled these things, these are our systems - can't be true - can't be true." Now, for example, the Germans, particularly on their diplomatic systems, the key word system which again was a 50,000 word code book, with a key book of 10,000 lines with a double encipherment. In other words, they would take the message which was in numerical code group, and they'd start someplace and pick out the additives and add. Then once that was done, they'd go to another part in the key book, take some more keys, re-encipher it by adding it twice. So, in effect, the total key was a key of 10,000 times 10,000 lines. And they used a separate encipherment system by indicating the line of the 10,000 which they used for first encipherment and the line that they used for the encipherment the

second time and then they had a daily key which changed to encipher this clue. That was this key word business, then they converted those numbers to letters which was a 10 x 10 square. This is a system the British called Floradora, because it had a consonant vowel, consonant vowel. Now, apparently the Germans were a little concerned about security of that system, too. They were concerned in the right place - there were concerned in Buenos Aires because the code clerk in Buenos Aires was a lazy son-of-a-bitch. Shouldn't call him a son-of-a-bitch, because he gave us a break into the system. What he would do, was, instead of, I think, following the implicit orders which would say "Select a starting place and go through and then at random select another starting place and go through," he would stick to a couple of pages which he preferred. He'd open them up early in the book, he liked those. What he did, he would write out the lines and then he would start the next line and write that underneath it - and have in advance the double encipherment, a long string. He was lazy, really. When he did his encipherment, he just took as much as necessary, then he moved over a little bit, took some more and moved over a little bit. So it so happened we had a four-part message from Buenos Aires in which, if you just shifted over the length of a line, which was I think, 50 digits or something like that, we had a depth of 4. We had had a copy of the code book because when the Germans were sending out material, they made a mistake, instead of sending it out with an official diplomat I think they had some businessman. They asked him, and the FBI intercepted this material. They said we have to check these things, and we got copies of everything. They tried to do it in such a way the Germans wouldn't suspect that the stuff had been photographed. We had good cooperation with the FBI. So we had the German key book, not the key book, just the code book. We had this depth and so we were able to start solving this. You know depths of 4 with a one-part code with Lutwiniak working on it. Things like that

\_\_\_\_\_ (?). Frank Lewis, there, Delia Sinkov was there, Frank Lewis, Bill Lutwiniak, Paul Dirsik was in that group.

FARLEY; Was Mary Jo Dunning there?

KULLBACK: She worked on the Japanese. This is when we had Deffenbaugh. We had quite a nice group by that time, so that we began to get some ideas of the system long before we had a complete picture of it. Again it's the old story, you know a little about - - in fact, we were working on the system, and we didn't realize it was a double additive, this code book, until later on. We finally got an idea of what kind of system it was, but we kept plugging away at it. The British apparently had gotten to know that it was a double additive long before we did. In fact, they decided it was too difficult for them. At least they had more important fish to fry, and they just even stopped intercepting the German diplomatic messages. But they had something and they didn't realize what it was. They had the first 25 lines of the key book, what the Germans called the "Tangent Tafel." Apparently, they had a spy of some kind in some of the German embassies and he had had enough time at one time to get to this key book and he copied the first 25 lines. Now this guy in Buenos Aires that I'm talking about - the lazy guy - he limited himself a good deal in this message to those 25 lines - doubles. So that once that we got our solution from the overlap and eventually when Sinkov and Weeks and the others went to England and brought back some of the stuff, they brought back the 25 lines. We were able to relate to two things and we saw how he was doing it, so at least we got a start. At least we got the first 25 lines and we had a picture now of what was going on. So that Buenos Aires guy was doing all these things, Buenos Aires messages were ideal. Eventually, the German in Berlin who was the head of their communications outfit began to realize that these things which were being done in Buenos Aires or some of these places, the way these cryptograph clerks were using systems, were not

distributing the key usage over the entire key book, so he made them use procedures. For example, he insisted that if they use line 1, 2, 3, 4 - for the other half they must start at line 4, 3, 2, 1, you know, for that. But by that time it was too late, we had gotten so far into the key book that early in '42 we were, we had recovered the entire key book. We were able to read those messages. But, when they questioned Buenos Aires about security, the reply was a very interesting one. He said this is absolutely secure. Then, of course, he was talking about physical security. He described the scene in which they had one room with only one door, no windows, in which the code books were kept and the way the work was done and there was a guard sitting on the outside with a police dog and a loaded pistol. Sure the physical security was perfect, but the cryptographic security was terrible. And the same is true with the Japanese. The Japanese apparently were very physical security conscious and as I understand it some of the code rooms that they had was in a room access to which was through steps, through a trap door in the ceiling. You had to get up to it that way, with no windows. I mean it was a very physically secure place but cryptographic security, the nature of their systems left much to be desired. And, of course, these are some of the weaknesses which enabled us really to accomplish what we were able to do.

FARLEY: Dale Marston asked me to ask you a couple of questions. When did you first learn about the German Enigma, is the way he put it.

KULLBACK: Well, Mr. Friedman had purchased and had procured a copy - but it was a commercial Enigma.

FARLEY: It wasn't after Rosen's return - you knew about it before?

KULLBACK: Oh, we knew about the commercial Enigma and the usage and we would have been able to handle if we had a volume of material in that commercial Enigma, because we had worked out things that could be done. In fact, we had problems

in ASA (SIS) at the time, which involved maybe solution of the message, or recovery of the wheels and the rotors and everything else. So we knew about the commercial Enigma long before Rosen came back with Sinkov with the information about the military Enigma.

FARLEY: How about the bombe? When did you first learn about the bombes?

KULLBACK: Well, I went over there in April 1942.

FARLEY: With Roy Johnson?

KULLBACK: No, no, no, Roy Johnson went afterwards, he went later on. I went after Sinkov and the others had come back. And the first stop I made was in Berkley Square, which was where the diplomatic section was located. They had moved all the military activities out to Bletchley, but Berkley Square was where they still had the diplomatic under – oh, what was his name? He had come to Washington? My memory has gone to pot. He was one of the British who had worked on the things in 1914 and they were working on the diplomatic systems.

SCHORRECK: (Suggested a name Kullback was trying to remember – “DeGrey”)

KULLBACK: No, no, DeGray was there. Dennis<sup>†</sup>! He was head of the outfit in Berkley Square. They were working on a diplomatic - - my first stop was with the group that were working on the German's systems and I brought things along and we exchanged. Even while I was there, it was interesting, just as sort of a routine everyday affair, in would come a piece of paper which had been picked up in the wastebasket in one of the German embassies. They still had these spies, and this was at a time when the Germans were getting worried and trying to introduce all kinds of variations in the usage of the key word systems – double key words. They couldn't get key books out to everybody at the same time and they were starting, for example, to provide - - they would write it out and go through some kind of transposition and stuff. What we got was a copy of the work sheet that the cryptographic clerk in the German embassy had been using and instead of

tearing it up he'd just crumple it up and throw it in the wastepaper basket. This was quite a big help to us in continuing, in keeping up with the German systems. And I went through that with all of the diplomatic systems which were in use - - Italian, German, some of the others. Then I spent about a week or two there with that group, particularly with what's his name? Philby who is now in Baltimore. He was in charge of them. And that quite a group of people. When Johnson went, I had come back and then he went to work with that group and while Johnson was there, we had gotten the last line, of course. I remember we sent Johnson a cable in which we said "We dood it." That was when we had gotten the last piece of additive out of that 10,000 page - 10,000 line German key book. Then from there I went to Bletchley and I spent a couple of months at Bletchley and there they took me around and showed me everything, the details of their operations on the German systems, where they set up the menus and the cribs and everything and then they took me to the bombe rooms. They showed me the bombes and how they operated and everything.

SCHORRECK: How did you feel looking at that and seeing that? Did you feel that they were so far ahead of us?

KULLBACK: No, I never felt that they were that far ahead of us because we had in effect accomplished, first of all - so far as the German diplomatic - that double key word systems was concerned, they had given up on it. And we had, in effect, gotten a solution so I had nothing to be ashamed of in that regard. We had solved the Purple, which was, I think, a much more difficult solution than the solution on the Enigma, because the Purple solution was done from scratch, with no clues, no devices, no nothing.

SCHORRECK: No captured machines.

KULLBACK: No captured machines, no captured material. All we had was the messages which were being exchanged by the Japanese and the State Department

cooperated by providing messages, copies of the messages, which had been given to the Japanese in which the Japanese, I guess, were then transmitting literally, so that we could have some cribs, but it was a solution with no captured materials. A purely cryptoanalytic solution, whereas, so far as the bombes were concerned, I knew that they had captured a copy of the German Enigma and they knew about the Stecker board and in general about the usage so that granted it was an ingenious idea of exploiting explaining the reciprocal wiring notion by setting up the cribs and just running, in effect, running an Enigma machine at a high speed through all of the possible settings to find a setting which would be consistent with – if A went to Z and Z went to this and this went to that, you found a setting in which the wirings would be consistent. I felt that the way you administratively, the way which they were set up, in which they had the group providing the cribs, the menus sending it down to the machine room to run. In fact, when I came back, we set a similar setup with the IBM room downstairs where we had punched up the 10,000. We would get a message and we could more or less say that if this was one which had been sent on a German internal radio system. They had, you know, the embassies communicated directly with Berlin. They also sent messages through the normal channels. The messages which were sent on the regular commercial channel, there was a heading and a signature. On the German network, all of this was encoded, so we knew that messages out of Berlin would be signed by the head of the German cryptographic office. So that was, those were clues which in effect provided us with the cribs. And the IBM machine room, we would give them a combined key of about 6 digits and they would run through the various combinations and found which the lines would give them those 6 digits. So we were operating with a German cryptographic system using the IBM set up as though they were the bombes, but in a procedure similar to what the British had

developed with their cribs and so on. I mean, in that I felt, you know, that it was a system which was working and effective, but I then have a feeling that, gee, you know, they were way ahead of us. I didn't feel that at all. In fact, in many of the things I felt we were ahead of them, like in the German key word. Granted in the Enigma they were ahead of us because they had the traffic, they had been working at it, but I didn't feel that there was anything for us to be ashamed of.

SCHORRECK: But, we've even got documentation from the British that says that. They couldn't work the four-wheeled Enigma and they gave that to us to do and we did it. We'd done such a good job on it they stayed with the three-wheel Enigma. They didn't even bother with it.

KULLBACK: You mean the one now, "Madame X."

SCHORRECK: Yeah.

KULLBACK: Madame X, in the basement. Yes, I say, it was interesting to meet some of these people that were working on the Gehemschreiber and, of course, Tiltman was a real gem and his capabilities. The things he could do all by himself and what he had done finding the books which some of the agents were using. They would use ordinary published either dictionaries, Berman/English dictionaries or novels and stuff like that and use a system in which they would get the key by picking out letters down the column on certain pages and stuff like that. He spent quite a number of hours in some of the libraries in Europe hunting for these key books and finding them. I mean, things like that, I mean they're impressive what they did, but nothing there was something that I felt that SIS had anything to be ashamed of.

FARLEY: How many people in SIS were privy to the British work on the Enigma? Was Rowlett, Furner, Small?

KULLBACK: British work on the Enigma? Of course, we had quite a large contingent stationed at Bletchley.

SCHORRECK: \_\_\_\_\_ (?) were sending the reports back, and so was Small.

KULLBACK: Yeah, we had quite a large contingent stationed at Bletchley working with the British on both I think the Enigma problem and then the Geheimschreiber, the Colossus, and so on. Oh, I guess most of the old timers at least in ASA (SIS) knew about the bombe and what they were doing on the Enigma and, of course, Martin was working on photoelectric ways of doing a lot of things and everything so that what the British were accomplishing with the Enigma generally wasn't known. I mean, we didn't see all the messages, but the fact how they read them and so on was no secret for many of us.

SCHORRECK: I don't think there was much cooperation between the Army and the Navy. The British Navy and the American Navy stayed pretty much tight.

KULLBACK: Well, of course, the Navy had quite a number of bombes that they had built. They were working primarily on a submarine problem, I guess, jointly with the – – well, there was really no need for an exchange of ideas or information because these were distinct problems and we in the Army had enough material and data to worry about the problems we were working with. The Navy had its hands full with the submarine problem.

SCHORRECK: Although Redman accused the British of holding us back for a whole year by not giving us solutions to the Enigma when, on the Sinkov trip when he and Rosen took all the stuff over early. Of course, Frank Rowlett says it wouldn't have done us any good anyway, even if they had given us the thing because we weren't that far along on the development. But Redman really got teed off at the British.

KULLBACK: I've read in there, too, statements that the British double-crossed us when we gave them Purple machines and they didn't. I don't think that's true, as far as I know. Maybe Redman was thinking in terms of solutions to messages and so on. But, they brought back knowledge about the Enigma. In fact, I think Rosen got

started on then getting a hold of -- What was his name? in the Bell Tele - Bell Lab - to build the Enigma. The solution, but to do it differently instead of with the stepping switches, instead of having like the bombe in which there were actual rotors which went around at great speed, actually have the rotors stand still and, in effect, move the machine around it, move the wiring to fix things. That's what the way Madame X worked, in effect. Now, maybe, maybe, it might be true that Redman couldn't get started in building bombes for the American Navy as soon as he would have liked to. Now whether it was because the British -- but so far as I recall, Sinkov and Rosen brought back to us --

SCHORRECK: Well, Currier was with them.

KULLBACK: Well, Currier and Weeks were with the Navy. In fact, I think they brought back the 25 lines. They hadn't really appreciated what that was and we had been working so -- again, it's the old story that you get into a little knowledge about the system if something turns up relevant to it you can exploit it, whereas, if you dropped the whole thing, you may have an important idea and a clue, but not know just how relevant it is, you see.

TAPE III, SIDE A

KULLBACK: So far as I know, they brought back information about the Enigma -- maybe not details -- but we knew what was going on there and at least, I know when I went -- well, by that we were already in the war '42. They kept no secrets from me.

SCHORRECK: The Navy was having its own problems anyway.

(b)(1)  
(b)(3)-P.L. 86-36

KULLBACK:



FARLEY: What do you think? Sir, we have taken three hours of your time. We'll have to come back. We still want to cover the pre-Pearl Harbor days, the 14-part message, the Winds message, and all of that.

KULLBACK: Well, that is something I'm not going to be able to help you too much with, because by 1938 when I came back, and they started working on Purple, we had set up a German unit. I was working with German material, Sinkov was working with the Italian material and then Rowlett and Ferner and that group were working with the Purple. And when the messages were being read, I mean, in

those days it was a small unit, and we saw practically all of the Magic Summary and the output was all distributed. We read these things. But my job was the German material, Sinkov's job was the Italian, so that we weren't as close to the – I knew about the 14-part message because we saw these things. At least in those days it wasn't so compartmented that we didn't know what was going on. I knew about the message decoder. I remember Schukraft showing me the message in which the Japanese here at the embassy was instructed to destroy their codes and we said, well, of course, that's going to mean war. Things like that, but, and I remember about that 14-part message, but my knowledge is really somewhat heresy, and a little bit, rather than knowing as much as I do about the work that was going on. And then it wasn't my business. If we can get together again some day.

FARLEY: Yes.

SCHORRECK: We need to go over that, we need to go over what you were doing anyway.

FARLEY: Yeah, in a little more detail. Next week, some day next week, or are you tied up?

KULLBACK: Well, let me check up, I'll call you. I think I have your number.  (b)(6)

so I don't know just what's going. I'll call you and get together again.

FARLEY: This is great, I mean, this has been tremendous.

SCHORRECK: this is good.

FARLEY: Can't you see all those gaps being filled in there?

SCHORRECK: There a lot of gaps being filled in.

KULLBACK: If the next time you come you have specific questions instead of talking off the top – try to answer specific questions.

FARLEY: I had some questions that I have just drafted – I'll just leave them with you. You covered most of them in detail. Up to about there (he shows him his draft) and then we would like to, as I say, go on as long as you wish.

KULLBACK: No objection.

FARLEY: Maybe the next time we ought to come in and spend the whole day.

SCHORRECK: Well, I would think if it would be all right we might get here a little earlier.

KULLBACK: Well, whatever, well, I'll talk to you, whatever we can work out. I mean it seems a shame to spend all the time coming down here and then you know, not taking full advantage.

FARLEY: Absolutely.

KULLBACK: You know me, I'll sit here and talk.

FARLEY: That's great, that's wonderful, that's part of what we enjoy. I've been sitting here in awe. Thanks very much, Sir.

(TAPE III, SIDE B blank)

TAPE IV, SIDE A

FARLEY: Today is 9 September 1982. This is a continuation of an interview with Dr. Solomon Kullback which began on the 26th of August 1982.

FARLEY: Let's pick up the interview with the discussion of the visit to GC and CS by Sinkov and Rosen.

KULLBACK: \_\_\_\_\_ (?) was a result of Rosen and Sinkov's visit.

FARLEY: When we first learned about the German Enigma?

KULLBACK: Well, there was a military use of the Enigma, yes. In other words we knew about the existence of the Enigma, the commercial version of it and the fact I think he had copies of the patent applications and we had the machine and we had worked out exercises to know how to recover wirings and all of that sort of

thing. But I guess the fact that the German military Army/Navy were using a version of the Enigma, I guess we didn't find that until we made contact with the British.

FARLEY: Which would be?

KULLBACK: Well, actually, I guess at least as late as Rosen and Sinkov's return and possibly a bit earlier. It may have been mentioned by Turpin(?) or Dennison when they were here before. That's it. I mean, if we had to pinpoint a specific time without being able to refer to -- I don't imagine any notes were kept of these things so it'd be pretty hard to - unless you'd talk with say, with Sinkov. He might remember more details about their visit, you see.

FARLEY: When they came back, did they give you briefings or was there a gathering of the group and they, Sinkov and Rosen, told everything that they had learned from the British?

KULLBACK: I don't know whether it was that there was one general meeting. Actually, at that time we weren't too big anyhow. But, yes, they brought back materials which were made available to the groups that were working on problems relative to the materials that they brought back and discussed more or less what they'd seen and heard and been told. Yes.

FARLEY: Was Leo Rosen able to reconstruct or build any equipments based on what he had seen?

KULLBACK: Well, Madame X, in the basement of B Building was, I guess, a result of the concept of the bombe and a solution that I think he, I don't remember who made out the design for it, but I know he was heavily involved and then worked with Mr. Williams of the Bell Laboratories because the whole damn thing was built out of relays, you know. I don't think it worked as fast as the bombe of the British were using but this was a big installation and, ultimately it was used on some odd kinds of messages which we were working on. I didn't remember

exactly what because I didn't have much detailed contact with the use of Madame X. But it was used on problems where I think there'd been some problems, some difficulty about getting them solved by use of the bombes. So it was sort of a backup. It was really more used as a backup than the one for actual day-to-day work like the British bombes and then the setup which the Navy had. Now the Navy had a setup of bombes which were, I think almost exactly a copy of the German bombe construction with the big rotors. The concept of Madame X, really to describe it, was that in the bombe you kept the machine stationary rather the end wiring and you turned the rotors and the Madame X in effect, you kept the rotors, well, not stationary, you turn the machine around, that was the concept. So, but that was obviously the consequence of the information which Rosen had picked up. When did we start building Madame X? I know that was a big job. You've never seen it.

FARLEY: It was probably destroyed. Was it?

KULLBACK: No, it was, now at the end it wasn't destroyed, I think, it was dismantled, really, because I guess the stepping switches and a lot of the other equipment could be reused you know, it was like, I guess, a great big telephone exchange, really, when looked at. Also, a lot of pressure had to be applied to get all of the necessary wiring, stepping switches and everything else, because you know, those sorts of things began to be rationed out. But the scarcity and I guess the telephone company wasn't too anxious to give away this equipment. Kept what they had and so. No, but it was dismantled. Well, okay, it was destroyed. But it was really dismantled and I just don't recall, -- Dale would know, because he was working with the then the superscritcher which was down in the same general area. The superscritcher was more electronic. Madame X was really electro-mechanical, so the superscritcher used to work in a -- I remember I used to take people down there and show them it and make the point that the

superscritcher operated about 10,000 tests a second whereas the electro-mechanical could run through about 10 a second. And the fact the superscritcher, which was again the special applications of solutions on the Enigma in its design and construction more nearly, well, definitely resembles what began to be the computers, because the design, the circuitry was very interesting, independently had been laid out by our engineers and then when we began to get copies of the computer which Norkert and Ekley had worked on for the Census Bureau, I guess. Their first, the ENIAC, I guess is what they call it, electronics with lots of tubes that was the big problem. It was amazing how much similarity our engineers found between their circuitry and their designs and what had built into the superscritcher. But that, too, was dismantled. That really was, to a certain extent, the beginning of the construction within NSA. Now this ran through the end of the war. The reorganization which set up the research and development division, and then many of the engineers who'd been involved in a design of the superscritcher, Moulton, for example, Roger Moulton, he was one and Bowman, too, I think, was involved in those things. The next step, they got on into the children(?). We had the group. I guess ABNER was our first and this is where ASA and, what was our next, Armed Forces Security Agency and its activities we had to get heavily involved both itself in construction. ABNER we did build. Atlas was built outside and then the Navy also had an electro--mechanical made from relay switches, a version of ATLAS just to test the circuitry, I mean the concept. That served for quite a while. In fact, ultimately it was turned over I think to logistics studies at the George Washington University and they used it as a computer also. The circuitry was essentially the concept of ATLAS, but it worked electro-mechanically rather than electronically. It didn't have the speed like the other one did, but the concept of the programming and how you would use it, so it was a very useful training tool

in that respect. And then we got on into a lot of contracts supporting research particularly in the high-speed memories, high-speed circuitry. I remember General Canine used to tell me if it was any sort of thing which would bring us up to, you know, a billion steps a second, things like that. He was pushing, he realized that the bottleneck really in the computer \_\_\_\_\_ (?) applications then were simply the speed of the memory and the speed with which the electrons travelled. If you could get things -- well, of course, the ultimate answer turned out to be these silicon chips, that was. I think a lot of the stimulation for some of that research and development for these things was partly due to the support from NSA. We had contracts with RCA, Burroughs, IBM, Bell Labs, and all aimed essentially at developing the technique for high-speed memory and cutting down to size the components because if you get things closer together, I mean, it reached the point where even their travel time of the electrons began to be critical.

FARLEY: We're going to bounce back to the later '30s. Dale was wondering, Dale Mar<sup>s</sup>ton, was wondering whether you knew about the work that was being done at Bell Lab and I guess he had?

KULLBACK: The work that was being done at Ball Lab <sup>e</sup> — well, which work did he have in mind?

FARLEY; Apparently that immediately after Rosen and Sinkov came back, probably the one which you just spoke about, that Rosen was in contact with some representative from Bell Lab and worked out the Madame X.

KULLBACK: Well, that was Sam Williams, yeah, and they worked out. In fact, I think then they, Sam Williams the engineer, supervised the construction while the thing was being built down there. I think it was built by -- I don't know, because I really wasn't in that aspect, but it was the Jap Army problem. But probably by telephone people, because it was like building a large telephone central,

telephone exchange. Also, we had working with us as a consultant, I think, I think he had retired then from the Bell Labs, Nyquist. Well, he was very well-known in physics in connection with telegraphic transmissions, the speed at which you can send dots and dashes over a telegraph line in terms of sine waves. That type of Nyquist's law. It was fundamental. He worked with us. Also, we did get some of their literature, for example, Shannon, his work on information theory which was carrying on what had been done by Hartley and Nyquist and the Bell Telephone Labs. We've got copies of the papers which were internal Bell Lab, distributed internally before they were ever published. As a matter of fact, I think they were treated as confidential, because I think some of them were in connection with the work Bell Labs was doing on their own or in contact or consultation with us on speech, speech techniques and how to get secure means for the encipherment of speech. What the telephone company was doing on a commercial circuit was just varying frequencies and stuff like that, wasn't really secure, it would keep the average person who happened to get in on the circuit from understanding it. But I think the Germans were able to read all of the transatlantic telephone conversations which took place because it wasn't very secure. And I think that some of Shannon's work was in connection with that problem, the encipherment. That pamphlet he wrote had to do something with cryptanalysis, cryptography applying his \_\_\_\_\_ (?) with information, notions to it, I think. Some of this I am aware because in recent years I got a call from somebody up in Lincoln, Mass. around Cambridge, MIT, and they were trying to piece together some of the early history of information theory, Shannon's connection, and what relationship, if any, it had with us at NSA, and they were aware of that early publication. Liebler and I had an information theory, so some of these people had contacted Shannon and tried to elicit his memory, his idea. So some of what I am saying stems not from my knowledge then, but

information that I had picked up. But I mean, it was quite clear that if you look at some of the work of Shannon in connection with cryptography, that must have stemmed from contacts that we had. We had very close contacts with the Bell Laboratories. They were very, let's say, willing to work along with us. One of the first heads of research and development in AFSA was a retired Bell Laboratories man.

FARLEY: What's his name?

KULLBACK: A. B. Clark. He unfortunately had a stroke and died within six months of his retirement from Bell Labs and coming to work in our place. And, as I say, Williams was...worked with us very closely with us on computers, Nyquist worked with us, Shannon did. So that the information, the resources, in the Bell Labs were available to us through contracts and contacts and I think particularly in connection with speech. A lot of the exchange and, in fact, in the microwave link we had between Ft. Meade to Nebraska Avenue, when AFSA, let's see, I guess, no with NSA by that time, it was NSA, I think. General Canine was already the head and we moved out to Ft. Meade. We had a microwave link from Ft. Meade to Nebraska Avenue, and that microwave link was to some extent patterned after developments in the Ball Lab in a sense that the speech was encoded into 32 levels and the coding that was used was one which had been developed by a Bell Lab man so that the sequence, I mean, you just didn't take 0001, 001, 01, so, but the sequence in which it went down was related to the speech frequencies and in effect what it did was convert the speech to off-on signals and then encode them. Once you got off-on signal, well, you know you can encode it even with a punched tape, you know. All kinds of ways. And then the stuff was transmitted, then reconstructed at the other end and you got good quality. And, in fact, you read nowadays in which they talk even with these spectra recordings, commercial music, the first digitalizing the speech, and then

doing things with it and then reconverting it back, you get, it turns out you get very good speech. The output, where some of the other things would just be done with the speech varying frequencies, and so on. Omitting segments, that was another idea. You send the speech, but you don't send all of it, you just cut it out, cut out pieces. You used to get speech but it wasn't real good quality speech. All of these are things which we used for security purposes through cutbacks. The Bell Labs were very helpful, there's no question about that. But dates and things like that, they're pretty hard to pin down now.

FARLEY: Well, that's all right.

KULLBACK: I didn't really get involved in some of these things until after the war when we reorganized and set up first it was ASA, in essentially three sections – CSEC, COMSEC, PROD and then R&D. I got into R&D after the war after the reorganization, so I had to catch up on some of the things which had gone on in those activities during the war without actually having an R&D section. That was Leo Rosen's branch. I don't know what they called it, C Branch or one of those things where they had the engineers and they'd had a lot of these things. And, so I was more involved with the research and development activities after the war and that went on on some of these things. Then we started developing a new line of equipment. The big problem then was to get an on-line equipment. One of our first projects, Barlow was in charge of that activity and actually John Tasker(?). I remember Barlow, John Tasker and I making several visits to potential, at least what we hoped would be potential, contractors to undertake developments for us of what ultimately turned out to be the AFSAM-9, which was a rotor device, but to encipher off-on signals for the on-line teletypes. I think that served a very useful, we had a lot of them in the communications center, was used pretty widely. There were very interesting odds and ends of things. I remember we visited Underwood Typewriters – – the big potential we

felt were in typewriter companies. And we visited Underwood Corporation. They had a factory of some kind, I think it was in New Haven, I know it was in Connecticut, but I think it was New Haven. They had a four or five story building where they did work in connection with their own developments also. There was one floor in that building vacant, absolutely vacant and it would have been a very nice ideal spot for them to have set up an activity doing developments for us. But it seems as though the manager of that part of Underwood, that building, was more concerned with maintaining pristine neatness and beauty of that floor. I don't think we ever did undertake it with them, but it seemed to us, anyhow it seemed to Barlow, Tasker and myself, that the biggest objection he had if they started doing that, the floor would get dirty and the place would get messed up. But I think ultimately, ultimately, that's where we went with Burroughs..

FARLEY: Oh, yes.

KULLBACK: I think it was a profitable association for Burroughs. I think ultimately, of course, the AFSAM-9 machines were produced in large quantities and did a yeoman service until ultimately they were replaced by whatever was next down the line. But, after a while, ultimately, I think you remember, Underwood went under. They were bought out by somebody else, and I think it was this sort of an outlook and philosophy on the part of some of their management, not the top management maybe, but at least the guy who was not planning too hard, apparently had enough power to decide not to get involved in this. They didn't have the foresight looking ahead to get involved in new sorts of things. That was a very funny incident, you know, I think if you ask Barlow or Tasker. I see him occasionally and recall the trip that the three of us made just to try to find the potential of some of these companies, and mention to them "Underwood." I'm sure they will never forget that. There's a question here, jumping around, it

says, "When did you go to England?" I went to England in, I think it was May, of 1942.

FARLEY: So it was after the Sinkov/Rosen trip?

KULLBACK: Oh, yes, it was after that, that's right.

FARLEY: Frank Lewis was a little confused on this yesterday. He thought you made the first trip.

KULLBACK: No, no. Actually, the first trips were made by the British to us. Our first contacts were with Dennison when we were still in the Munitions Building and then Tiltman came over. Now I think their visits to us were also the – though you may not have been I don't think we were aware of it, of visits that you read in some of these books nowadays that cover these things. Part of a British mission in general which came to this country to try to get some kind of understanding and agreement with the United States about what kind of support they may get. There was a lot of Lend-Lease things going on so Dennison and Tiltman may have been, I don't know, may have been really theoretically officially members of those groups, or they may have come over as individuals after some understanding had been reached, that we and the British would exchange information. But, the next visit from the American side, I think, was – I was the first one after that. Then after that I was followed little by little, a large group of Navy people and Army people, but I went there in May of '42 and came back in August '42.

FARLEY: You were there that long. What sort of a mission or task did you have – what were you to do over there?

KULLBACK: Visit and learn everything. I really had no formal piece of paper which said do this, that and the other things. It was essentially really, go over there, see all you can about the way in which the British were functioning, learn as much as you can, pick up as much as you can in the way of documents, captured code books,

copies of these things, and come on back. Also, well, I'd love the paper work. I think my orders specified three months and shortly before my three months was up is when the British – I don't know who it was – Tiltman or some of the others called me in and they showed me decodes of the German Geheimschreiber, the teletype link from North Africa to Berlin. And in there they were quoting from the messages that our military attache in Cairo had been sending back to this country, which, of course, seemed to prove that somehow or other, the Germans or Italians, of course, they were working together, had been able to read the messages which were being sent. And, Feller<sup>5</sup> was the person. One, I guess, was to let me see in those messages the fact that Feller's messages were being read. Because the British were concerned about the fact that these messages were giving the Germans, instead of information about things, British plans. And, of course, it turned out to be. He was using the MI-10, we had, that was one of the, one of the few codes that we had compiled and actually was ever put into use, because the division field codes and the other codes were all made obsolete once the SIGABA and the Hagelin device were introduced. They were preferred, obviously. They could do things the codes couldn't. So I immediately sent a cable back on the secure circuit and communications system which I could use, to Washington about this. And, of course, Friedman, whoever else was in charge there, they didn't stop to say this was a secure system, "we've just put it in." You just don't believe it and I guess it wasn't long after that when Colonel Hiser, well, he was then Major Hiser I think or captain, whoever, what his rank was, was on his way to Cairo with the SIGABA, big machine, and once that was introduced, all of this information ceased. Now what the relationship is between the fact that the Germans couldn't read any of this material anymore, and the fact that it was long after that that, what was it, Montgomery pushed Rommel, kicked him all the way out. I would believe that there was some relationship between the

improvement in the security and the, at least the capability to defeat Rommel. But what I was getting at was, I was asked then to stay over for another two or three days, you know, to follow up, make sure, on these things, so in effect I ran over the stipulated length of time in my original orders by three days.. So when I got back, I put in the voucher for per diem and all of these things. I asked for the length of time, that had been covered by my orders, and then the three extra days. Well, eventually, stack of papers, six inches thick...

TAPE IV, SIDE B

KULLBACK: ...was built up, I think it went up as far as the Secretary of War. I saw that stack, but their final decision was that I was not entitled to the per diem, you know, whatever I had been asking for, which, for those three days, because my orders specified I was to go there for a period of 90 days, and I didn't get a formal supplement to my orders, extension of my orders. It was just checking back with ASA and they told me to stay over until this thing was all cleared up and so on and which I did, but apparently the War Department, or was it then the Department of the Army, yet didn't, or at least, the Inspector General, or whoever got involved, just didn't think that that was a formal enough extension of my orders. There's a letter in here. How come (Question 18) "As chief of the Japanese section in SIS, why didn't you become the American Deputy Director of Central Bureau in Australia?" There's a very simple answer. While I was in England, is when General Akin, who was then with MacArthur in Australia, sent in a request for, I don't remember whether it was specifically for Sinkov, I think it was specifically for Sinkov, and whenever additional personnel to get together and be sent out to Australia to start doing cryptanalytic work – you eventually.

FARLEY: Yeah, that's right.

KULLBACK: Now, when I came back in August, I think Sinkov had already gone, so one reason would be that I was in England at the time, and actually we didn't set up the Jap Army activities at B-2, at Arlington Hall Station, until after I had come back, and I think Sinkov had gone. So I wasn't really head of the Japanese section and he was there. These things occurred and sort of parallel with that one. Then I have always suspected, have no way of proving it, but, you know, you want these little gems. When Sinkov went to England with Rosen, General Akin, I guess he was Colonel Akin at the time, he was head of the SIS and since we went not in the war, the idea was you be put on active duty. We were reserve officers, Sinkov was a reserve officer, I was a reserve officer, we could be called to active duty for, you know, so you have a military rank, I mean go as a military, not as a civilian in connection with that job. Since we were really not at war, and this would have been being sent to what was then considered a dangerous area, because of all of the bombings which were going on in London at the time, I was asked to check with my wife and see whether she would have any objection, you know, if I were assigned to this trip. Why they did it, well, I don't know. I guess because it was sort of a mission into a dangerous area in peace time. I guess we were reserve officers, I mean, I guess regular Army wouldn't have to. At that time Leo Rosen wasn't married, so he had no wife to be concerned about. Abe wasn't married then either so he had no wife who would be concerned, and then, of course, my wife said, "No!" She wasn't going to have them send me out to London where the papers here were filled with daily bombings, and the night bombings and how many buildings were collapsed and people killed and so on. She said, "no," so I had to come back and tell General Akin that I was sorry, you know, I couldn't. If it was a matter of choice, then I had to say "no", so then he selected Sinkov, and I think he sort of remembered that thereafter. Consequently when there was a question of

getting somebody to come back to work out there in Australia, he asked for Sinkov and not Kullback, but in any case, I was in England, well, that wouldn't have made any difference. They could have waited, I'd come back England and then go out to Australia. But, I always have felt that that was probably the reason that Abe spent four pleasant years out in Australia, and I spent it in Howard County. It was just that, I guess, Akin remembered and maybe resented the fact that he had asked me, and I had to say, "no, I can't go."

FARLEY: That's a good explanation, I'd like – that certainly makes sense.

KULLBACK: I think it does, I think it does.

FARLEY: No, that has always bothered me, why you weren't sent there.

KULLBACK: It wasn't the question as chief of the Japanese section, why didn't you become. Actually we had no Japanese section at the time. When I came back, I still worked with the group on the -- we had really finally reconstructed the entire keybook on the German diplomatic system, what was what you call GEC, I guess. The key word system, and it was not long after that that Sinkov went down to Australia, some more people went along and beginning to get contact with the Japanese military, or at least we had then intercept stations in range of the Japanese Army transmission. For one thing, as they got farther away from Japan and had to communicate back to Japan, they had to increase the power of their transmission. We began to get traffic, that once we got enough traffic, then B-2, which was the Jap Army section, was set up and I got into that with Frank Lewis, Lutwiniak. A lot of the basic group we had which had originally worked on the German key word system. Because by that time, that was under control. We had the entire German key book, the code book, we knew who was sending what to who, as a matter of fact, I think I mentioned last time. That we then set up a link with our IBM section and communicated with them, almost parallel to what I'd seen the British do in Bletchley in connection with the menus that they had made

up to send to the place where the bombes were and running it and getting it back and do all of the translations afterwards. It parallels, a very close idea. But then the B-2 was set up and since the heavy initial reconstruction of the code book and the key book especially, was all finished, Johnson had been in England. After I had come back, he was sent to England, and it was the wrong Johnson, too.

FARLEY: You know that Lewis mentioned that yesterday.

KULLBACK: There were two Johnsons, and I think originally the orders were for one of these two Johnsons to go to CBI, and the wrong one got the orders and went to CBI. The other Johnson went to England to work with the British group there for awhile, you know, liaison. But, it was the wrong Johnson, who ultimately went to CBI. I think his wife was very happy about it, because she had told me before they got married that he was going to marry her. She was going to get him, and he was going to marry her. She was a short, happy, pretty little girl, he was tall. She had made up her mind that he was going to be her husband and eventually that was what it worked out. So I guess she, I don't know if she ever knew about the mistake about the wrong mistake that the wrong Johnson went to CBI, but it was to her advantage because he came back and she had the opportunity to get together, and they got married.

FARLEY: Didn't you work on German Clandestine or Agent communications when you were...

KULLBACK: Oh, yes, we worked on all whatever German traffic was available and this was the diplomatic, GEC and then there was a lot of communications really Clandestine Agent traffic. Frank Lewis was up to his ears in that sort of stuff, from South America. And some of it was picked up by the equivalent to the Federal Communications Commission. They were monitoring. Some was picked up by FBI because this was espionage obviously, and it came our way, and there

were all kinds of systems. One system we eventually discovered involved the use of a dictionary. And what they did, they would give the page number. This was a dictionary which had two columns. They would give the page number, whether it was the first column or the second column and how far down on the page you had to go to find the word, so they would transmit a number but that would be page so and so, column one or column two, and you count down and that was the word. That was the code book, and, of course, it's a good system for an agent because, I mean, you have a dictionary around and nothing suspicious about it as if it would be if it were a definite code book. That was one of the systems Frank Lewis worked on. I think eventually once we realized what the system was, we could begin to break it as a code because it was under one-part code, you see, you know the pages and down the columns and I think once we had some reasonable idea of words, their locations, I think somebody hunted through libraries for various dictionaries involving German or Spanish-German, I think we ultimately found. This is one of the things Tiltman did long before the war. There were a lot of such systems which were used by the, I guess the German agents in the war, and they had to be systems so that the man traveling, if people looked at his luggage, there'd be nothing suspicious about it. And he spent a lot of time, he used to, he told us, in hunting through the libraries or the bookstores in Paris, trying to find a specific book which was being used in the means of communications. And we had quite a number of those things. Also, cipher systems, transposition systems, substitution systems, they were a lot of fun on those things. Then, in fact, also there was one in which, remember that, an agent named Felix, that was his code name, was sending messages and what he used was a standard commercial code book with a Holtz code, a German Holtz code, which had been developed for use in connection with lumber industry. But the thing about it was it had two versions. One was in German and then one

was a version in which the words, the meanings had been translated into English, so theoretically somebody could compose the message in German and you could use the English words and hopefully make sense out of it. As a matter of fact, it was that thing which convinced me and nobody has been able to prove otherwise, the fact that mechanical translation was not going to be very successful. And you see this was, in effect, a means of translation, because, you could write the message out in German and code it, and at the other end decode it presumably with the English meaning. You'd get, really it was amazing how you'd get messages which were difficult. Now if it was a simple message, but then you really wouldn't need to go through this translation alteration(?). If it was a real message you have to get it in the language in which you sent, not in the English. So if it was sent in English, the original message, English use of that code, then you'd have to really decode it in the English version, or German, but if you tried to go from the English version to the German or vice versa, it wasn't...Now this guy Felix used that code, but he used it with a really sort of a sophisticated encipherment. Again, you see, it had to be a sort of encipherment which he didn't have to carry extensive keying materials with him and so on. But, we read in one of the key words systems, the German diplomatic system, a complete description of how Felix was to encipher his messages in the Holtz code. So we finally began to get these messages, and we said this is Felix, and we put the two together. We were able to read all of those messages, too. The next time you see Frank Lewis, tell him Felix, and I'll bet you he'll know what you're talking about. There was really nothing spectacular, as far as I recall in that traffic, but at least the FBI, the people who were concerned about such things had a pretty good knowledge of what they were dealing with. A good deal of it was information about shipping. Ships leaving port and coming to port which ultimately I suppose found their way to the German submarine fleet to alert

them to what this traffic was. But, as I say, there was really nothing spectacular. You think, well, here these are secret agents they're going to do all kinds of work. It wasn't that spectacular, but to us cryptanalysts who were interested in cryptoanalytic problems, were a lot of fun working with them. It's kind of funny how, in the units where we were working solving these things, as cryptanalysts how our interest was more in the cryptoanalytical problem rather than in what the messages were actually saying and who was doing something about it. When we got on to the Jap bombe we were a little bit more concerned with that because actually the intelligence people and the translators were right there. First of all we had, I don't know, but I would guess, our setup in Arlington Hall would have resembled considerably the setup in Australia. We were doing, because we did have an allocation, we would work on certain parts of the keybook. New people working on it and we were exchanging information all the time and we had, you know, as you look at it now, it was, I think, a very remarkable cryptanalytic achievement. I think very few people are aware and appreciate the fact that here was a relatively sophisticated cryptanalytic system using a code book, and encipherments in Japanese. In the foreign language. That we were able to go out -- the recruiters -- young Army boys we used because then the girls that we recruited would come back to Washington and think they were all going to get husbands that way. And literally in a lot of cases these barefooted girls from the hills of West Virginia were brought in and given some training. Also, some of the reserve officers who had gone through ROTC, and the OTC and a lot of enlisted men, were given a course of training. Frank Lewis, Lutwiniak, no, I think he eventually ended up in CBI, but Frank Lewis, Dehlia Sinkov, Sam Hall and a couple of others.

FARLEY: Was there Dillinger there, do you remember?

KULLBACK: Yeah, Dilly was there, year. Wrote up really training phamplets, training courses and we would get these new people in and teach them about the Japanese system and a little bit about some of the basic words, the common words, and turn them loose on the overlaps. And the IBM equipment would run through some of the frequent code words which would have occurred. Then they would recognize the depths and if they had any questions call over one of the translator guys, and he'd say, "Oh, yes, these things are good." And this was done, as I say, by people with no prior knowledge of Japanese, no previous training. They were really given a relatively short training course, and the job had been broken down into simple steps and pieces so that these people could grind out and, in fact, what we had in B-2 and in - you people - the equivalent of all the communications of the Japanese Army and Japanese military setup. I guess you may have not been aware, we had them functioning in Arlington Hall. The translators were the next wing, so we had close contact system and also some translators were assigned to work on the overlaps, so that if the people trying to find the key, this is when we were reconstructing the key books. And any questions, they could call these translators. They would move around. Also, in the area, I don't know whether they were with the translators or another section, were a group a really the G-2 people. The story was always that what we turned out was raw data, so to speak, and this had to be the processed before it really became intelligence. And I think they kept the battle order there as well as in the Pentagon. The one man I remember in particular, well, there were two men, one is Edwin Reischauer. No, wait a minute, yes, he had been the ambassador, and his sister-in-law I guess it was, also worked with us in B-2. She handled records and files for us. And, of course, Alfred Friendly, who then was editor of the Washington Post. I remember on one occasion to cheer up the people who had been working on the cryptanalytic side, because after a while,

you know, working three shifts a day particularly those on the swing, late shift, what the shift from midnight to eight a.m., that was always dark, you know, especially in the wintertime, what'd they call that; there's a swing shift, the graveyard shift. Some people preferred to work on the later shift because if they had children at home it would give them the day with the children. So anybody who wanted to volunteer to work on those shifts was always welcome. Otherwise we used to rotate, you know, and give people time off. Occasionally they had to feel that they were not being neglected. Frank Lewis and I, we would come back and spend many a night working down there. At least showing our presence to make them feel that, you know, they weren't completely forgotten and ignored. It's funny how these sorts of things develop. Even though they knew what they were working with and how important and vital it was. But one time, Alfred Friendly, I think, came in and we got everybody together and he gave us a most interesting lecture about how what was being turned out here was being used, and its significance. It was a very, very stimulating morale booster. At a time when you know, when people had gotten worn out and tired. Now you people in Australia didn't need morale boosters, or maybe you did, I don't know. I don't know. Slip Swears came back after six months out there with a story about some of the people out there that felt that their morale was low. Not insofar as what they were doing as successful was concerned, but they were so far away from Washington. They thought they'd been stranded out in the desert island, so to speak.

FARLEY: Well, we were always in competition with Arlington Hall, too, whether it was evident or not.

KULLBACK: Yes, there was sort of. Again, I don't think I mentioned this ever. It's never been brought out or discussed, but the solution, that first solution on 2,4,6,8. Were you there at the time?

FARLEY: No, Sir.

KULLBACK: Okay. We had accumulated the first Jap Army material that we had a lot of traffic on we had accumulated was 2,4,6,8 which was the Jap Army Water Transport System. And we had set up, I guess Corderman, who was head of SIS, General at the time, with whatever people and so on, apparently realized that it would be necessary, we had set up quite a communication system between us and the intercept stations and CB in Australia, so that I think all of the 2,4,6,8 intercepts we got, copies were also available in Australia. CB was working on that stuff trying to arrive at solutions we in Arlington Hall Station were working. This is when we were really a small group because we didn't know what it was, built up afterwards. Now, the solution was arrived at almost simultaneously in Australia and Arlington Hall Station. The relationship between the indicator and the group count and the time of day, that was used for the determination of the page and the row and the column and the row-column was repeated so once that was determined, and I think the first 2,4,6,8 used the square for the encipherment to the indicator but the body of the message itself they used no arithmetic. There was little later on, that next edition, so they changed and started using the enciphering square instead of normal arithmetic on the body of the messages also. And we got the solutions, we began an overlap and got the first idea. We knew we were there, and called General Corderman in to tell him about it. His first reaction was, lock the doors, pull down the shades, lock the people in there, don't say anything to anybody. I had to argue with him and convince him that that was the wrong thing to do. In the first place, we had this group out in Australia. They were working on it and if they got the solution, they would undoubtedly send us that information plus, how the hell would it look if it turned out afterwards that we had gotten the solution and had failed to notify the people out in the field what it was so that they could start doing

what they had been sent out there to do. So he realized that later, and so we prepared a message to CB to say what we had found and so on. Then if those two messages didn't cross, the one from CB to us and one from us to us, if we hadn't told CB our solution so that the two had crossed, I don't see how we could ever have lived down the statement, "They did it all!" And then, of course, once that was done -- the initial steps -- we allocated that CB would work on this part, we would work on this part, and the whole thing began to fall apart. Then thereafter, God, the keys and the day's output were being enciphered and shipped out, sent and vice versa. I don't know if the Japanese ever suspected what was going on in those links, but those were pretty busy links. reconstructing the code book every time a meaning was determined so that...

FARLEY: This was in mid '43? Early '43?

KULLBACK: April '43. I don't remember what day of the month it was, but I know it was April '43. If one could get into the files of old traffic, if the actual day of the month, but it was April '43 was the anniversary, and naturally, of course, the 40th anniversary of that is coming up next year. I think maybe NSA should think of the occasion to celebrate that fact, because thereafter, thereafter I think we began then to recruit, we had a lot of people and we then went on once the 2,4,6,8 was well under control, our cryptanalytic group started working on the 6,6,6,6, which was air system and then the administrative system next. It was so funny how the translators worked. Ken Lorrell, he was head of the group. They were getting so much to work on in the 2,4,6,8, getting a lot of battle order. They were so pleased with it that as far as he was concerned, forget it, don't work with the administrative systems. But once we were able to start providing them with the information from the administrative systems, which was a hell of a lot more important, although the Japanese military had a funny set up. When a unit came from someplace in Japan, the reinforcements, the supplies, all the

information about that unit would go back to its home base, I guess as well as within the military. Now then when the administrative system started producing they were all for dropping the 2,4,6,8 because the administrative system provided a kind of information which wasn't available from the Water Transport System. Then when we started getting into the Air Force system, eventually they were very happy and they had all of these systems, and as I say, between our knowledge about the communications which we built up from the material we were reading, also, within B-2, within the Jap Army section, for our own needs, we kept track of the units and their communications.

TAPE V, SIDE ONE

KULLBACK: For our own needs we kept in B-2 under Bill Erskine a small unit which kept track of all the units and their communications. Not so much in the sense of the battle order arrangements which the Pentagon military were concerned with, but so that in starting in overlaps getting keys recovered, if you had the material and you want to decipher, get some idea about the new keys, then if you could get a crib for some of these things it would be a helpful break into it. So we kept a record of the serial numbers of the messages from the various units so that it was possible that if we had a message from some unit, if we had the address code book, that we could have a pretty good clue as to the serial number of the message and the serial number was the thing that they started out at the beginning. They put the serial number, but that was encoded and then ciphered, you see. So that was a very useful clue, so we kept fairly comprehensive, so we had a pretty good picture for our own cryptoanalytic needs of the communication system of the Japanese Army. Of course, the intelligence people looked at it. From these same messages they got the

information that they needed for battle order and, of course, out in the Pacific I guess they had their exchanging, they had all of this battle order and, of course, say the nature of the Japanese military set-up in which casualties and so on were always reported back to a particular place in Tokyo so that you could tell if you break the messages. I mean, if you didn't have information let's say about the origin or destination because maybe call signs had changed or hadn't gotten into that address yet and so on, but the links, see if you knew, if you knew if it was going to this place in Japan, you'd have a pretty good idea what unit it was because by that time we knew which units had come from which places in Japan. Or if you knew the unit and it was communicating with Japan you would know where it was going to in Japan. Now, for example, all of the information about their casualties were reported back to those places so that that way not only was there information about battle order, but also about the strength of the forces, because these administrative messages covered numbers killed, wounded and all of that business, which was also very important to, I guess, the people that were fighting there.

FARLEY: Was there ever any tactical information passed at all or was that would that have been in different systems?

KULLBACK: Well, what do you mean by tactical information?

FARLEY: Plans for an attack on a certain island or an aggressive act by the Japanese against an American force someplace.

KULLBACK: Yes. Yes, as a matter of fact, I think it's mentioned in this book. (Kullback is now referring to some paperwork he is holding). Most of this book is really devoted to the Navy activities prior to and after Pearl Harbor and the Midway business. And, of course, the Navy had traffic and so that it was fortunate that they had the solutions of the Japanese naval code. Lewin doesn't seem to realize that on the Army side we really didn't get any volume of Japanese Army traffic to do

anything with until afterwards, later on in the war. But he went through the files of decodes which were made available a couple of years ago in the archives, something like that, and he mentions in here specifically about one group which had been bypassed. The information that was being fed to General MacArthur locally from CB what we had here, was planning a breakout. I hope I can – I don't know if I can find it – I don't know if I can specifically, but he describes that if it were sometime in July, I think it was probably July 1944, that this unit was going to try to attack. Now this was fairly large, I think divisions, divisional strength, was going to try to attack and breakout and maybe get off the island. And they outlined in complete detail, you might say, their tactical plan. What units, the order in which they were going to appear on the battle front, which units would be in reserve. How they planned to do it, when they planned to do it, down to the exact hour and second of the day when they were going to start the attack – complete in every single detail. And this thing we had gotten, oh, several weeks before the day was going to happen actually, it so happened, and we knew what these messages said. I was always curious as to whether or not what had actually transpired. We didn't have too much feedback from the intelligence, and from the actions which took place, it was all, all went out so to speak. And Lewin mentions this in the book in some detail and with a very interesting comment to the effect that when you know exactly what the...

FARLEY: That was from the administrative system, or was it in the Water Transport System?

KULLBACK: Oh, no, it wasn't. It was the administrative system. It wouldn't have been the Water, because the Water Transport System was used primarily to first of all, to control the shipping which then the Japanese had to go all from Japan through the various islands, the whole Pacific. And, for some funny reason, I guess, I guess this is the way – – you know the ships would have to give their daily

position, their daily noon position where they would be, not where they were, but where they would be. Also, it dealt, I guess, with the cargo and stuff like that so the 2,4,6,8 didn't really cover tactical or strategic other than the fact that I guess the movement of the ships with personnel and supplies were tied in with the plans and strategy of what they were planning to do. I don't know whether Lewin is aware of the difference between the Army, well, we would call the water supply system, and some of the naval systems, because this was definitely not a Navy system, it was an Army system. The information dealt with shipping, so that information used to be turned over to the submarine commanders. What nicer bit of information would be necessary for a submarine than to know that the ship was supposed to be at a certain spot at a certain day. And, of course, all kinds of ruses were used to make it appear that the information came from sources other than the Japanese communications systems. For example, if airplanes were available and they knew, they would make sure that the airplane would be seen or spotted so if the submarine hit the ship they might assume that it had been attacked because of the information from the airplane. Also, we had messages which were amusing to read, about all of the intense investigations and checking they did for sea/coast watches. They felt that all of the islands and the coasts were infiltrated with spies who were probably sending information about the shipping that they saw and all of that business. Some of the measures they took to avoid that were fun to read about, when I had nothing to do with that. And, of course, actually as I understand it also, we never got, this is all hearsay, but some of the submarine commanders had gotten so used -- they didn't know the source of the information, let's say, but they knew they were being informed that a ship or convoy was going to be at a certain place at a certain time. And apparently they got so used to the accuracy of this information that if somehow or other sometimes the ship didn't be at one exact spot, was

five miles off they would write communiques back and complain about the fact that the ship really wasn't where they said it would be. It was five miles off something like that. But, of course, it's been fairly well publicized now that within a year practically the entire fleet which the Japanese had, now not the, this is not the Navy, but the fleet in which the Japanese Army had to supply the troops out in the field and so on was practically wiped out. And then, of course, they resorted to trying to get supplies, information to these isolated units by submarine and all of that information was available one or the others of the systems.

FARLEY: You cited one example where four ships left Japan for Wewak?

KULLBACK: Oh, that was the first one. And that was the first message yes and this was after we got into it in April – July '43 – the first, one of the first messages we had was that they were going to be so many, I think it was four ships in Wewak Harbor, and that information was made available. I didn't know whatever was going to happen. I remember listening on the radio one Sunday around then. The announcer saying that the Army or the Navy – – somebody had reported an attack on Wewak Harbor and they had sunk four ships.

FARLEY: Made you feel great!

KULLBACK: That was a pretty good feeling. That was so far as I am aware, the first actual result of what we had been doing. Now little by little the pieces got so, with all of the battle order, that I guess MacArthur's headquarters had as good a picture of the Japanese military set-up as he had of his own. I'm just trying to find this item. (he's looking in a book)

FARLEY: I thought that book [Lewin's] was terribly inaccurate. I think they gave a page and a half to CB.

KULLBACK: Well, most of it, you see, was really devoted to the Navy side. And, if you look at this sources of information, the people he quotes were mostly Navy people, so

that on the point of view of security the Army was still more secure even at this time than the Navy because much fewer Army people talked to him, so to speak, to give him insight and background which wasn't available from what he had, were all the MAGIC Summaries. I guess sometimes he couldn't distinguish as between whether it was Army traffic or Navy traffic. All he could see was the messages themselves. So this is why in a certain sense his discussion of the military, CB, Army, Arlington Hall Station and all that, is well -- he just couldn't get that information and none of the military people really apparently gave him as much background as some of the Navy people did.

FARLEY: What did CBI contribute, the people in India? What did they contribute to the war effort? They were sort of stepchildren in one respect. I never read much about what they did.

KULLBACK: Well, they didn't work on the high level systems, because I guess either this was a decision made on a high level. They would do work primarily on the transmissions below the divisions and these were more like what the German field codes, you know, what we had prepared - divisional field codes, I think there were 3-digit systems.

FARLEY: Oh, were they?

KULLBACK: Yeah, and encoded. And there wasn't too much traffic.

FARLEY: Any air/ground or air/ground liaison code 0,1,2,3, I believe it was? Were they working on that? I think that was the air code.

KULLBACK: The systems they were working on were the lower level ones.

FARLEY: Yes, okay.

KULLBACK: You asked Lutwiniak -- he was there? It was tough. They were always complaining to us about trying to get help from Arlington Hall, but that's why you don't hear so much about CBI. They were working on the traffic, really low-range, I mean, the transmissions were being sent with low power. They were up

close, they could copy that traffic and it wasn't as voluminous as the higher level systems. It didn't cover so much, and I guess there wasn't so much material being captured. So they really had a tough job of it cryptanalytically. And, they were furnished with, I guess, whatever information was pertinent to what they were doing, but they didn't work on the water system or administrative or any of the other things. The two outfits who worked on that were Arlington Hall and CB. Of course, CB was essentially working for MacArthur.

FARLEY: Were they supporting MacArthur? Supporting that military command, CBI? Or was it a command in China?

KULLBACK: Oh, that was it. The China Burma India Theater?

FARLEY: No, but were they supporting the U.S. element in China or were they providing their intelligence to others?

KULLBACK: Oh, no, there was a U.S. military presence in China, yes.

FARLEY: Yes, okay, that was the command they were supporting.

KULLBACK: That's right, they were supporting the China Burma India Theater and CB was essentially supporting MacArthur, plus, we presumably were supporting the Pentagon, the staff, plus MacArthur. Because as I understand it at least, put it this way, cryptanalytically, I don't know about what went on with respect to their military planning. But whatever cryptanalytical information we developed was forwarded to CB and whatever cryptanalytic information CB developed came back to us, so there was always this exchange of "tea" and so on, and actually there was some reasonable allocation so we didn't all concentrate on the same pages and neglect the other pages. I wish I could find that.

FARLEY: How did SIS, Hawaii fit into this picture? Did they have military organization to support?

KULLBACK: No, all we had was intercept stations.

FARLEY: But they were not producing or processing.

KULLBACK: No, just an intercept station. We had no outfit doing cryptanalytic activities other than the units which accompany the various armies in Europe which were supporting them.

FARLEY: RI Company type?

KULLBACK: Yeah, the radio intelligence, plus. They did certain amount of cryptanalysis in Europe, but in the Pacific so far as I know any of the cryptanalytic activities of the high-level system were concentrated in CB and in Washington and CBI (China, Burma, India) theater worked on the communications of the units that were facing them, which were under divisional, regimental and this sort of thing. I mean out in the field, those were to a certain extent difficult systems because there wasn't that much volume of traffic, you see.

FARLEY: Were the British handling a lot of the CBI intercept? Because Lewin mentioned, I think he calls it WEC in Calcutta or one of those places.

KULLBACK: There were some interesting British training of Indian intercept operators and we were getting intercepted material from them. I think these people were trained so that they could recognize the Japanese radio signals. The Japanese had selected ten signals, they didn't use the normal digital signals. They picked ten signals. I guess those which were short signals to represent the digits and they were using those for their transmissions. As a matter of fact, these were some of, I think, letters that they could be read as letters rather than digits, but there were only ten of them. And these were the signals with shorter combinations of dots and dashes because in the Morse code, the digits I think had longer combinations than the letters themselves. So they arbitrarily selected ten signals which were used. Theoretically this was also a problem we had to solve which was 1,2,3,4, those numbers. Then actually, it's amazing. I always felt that our American communications would probably never been to able to ever accomplish it. But, in the middle of the war, they decided to change the signals

which they were using for the numbers instead of one set of the equivalent of ten letters which would represent the numbers beginning on a certain date, they were going to introduce a different set of letters to represent the ten numbers. Now, of course, if we didn't know that that would've fouled things up. But, of course, the usual thing happened. Somebody sent a message in the old scheme when it should have been the new one, so the people at the other end complained, so he retransmitted the message. So it was easy to relate the digits, and thereafter we had no trouble. We just converted to the proper numerical sequence. In other words, this was you might say an additional encipherment system imposed on everything by using ten arbitrary symbols to represent the ten digits system. This is what it meant. But, again, it was one of these things which and yet you see what they had to, first they had to educate, train the Japanese operators to recognize these. Learn that this is now 1,2,3,4. But as I say, what often happens in a big military organization when there is a radical change, somebody fails to get the message and doesn't make the change at the right time. So it happens, you get a message in the old system and the repeat of it in the new system. This used to happen here, to. But as I say, with the respect to Lewin. Apparently also you get the impression from this thing that Lewin was not a MacArthur worshiper.

FARLEY: Very obvious, right.

KULLBACK: He didn't think too highly of MacArthur and also maybe you get the impression that he feels as he looks back now on the MAGIC traffic, with the volume of information which was available to MacArthur, for his planning and so on, that maybe it wasn't purely MacArthur's genius which was operating but maybe MacArthur's ability based on a tremendous amount of information.

FARLEY: Did you get the feeling that all we did was help the British win the war? I mean in the Pacific for instance – but the U.S. was just also there, and the British contributed most of the intelligence?

KULLBACK: From this book? No, I don't think so. I think he, of course, he can't forget he's an Englishman and writing about a war in which the Americans and the British worked together. But I think so far as the Pacific is concerned, I don't think he attempts to play down the contribution of the American cryptanalytic solution to the whole thing there.

FARLEY: I didn't think he gave it enough pages.

KULLBACK: Of course, so far as really the Army is concerned, there was so much more publicity I guess about the Jap Navy systems. I know he tried. For example, I got a letter from Bill Bundy. Lewin had contacted Bill Bundy and he was looking interestingly enough for information for when the first solutions were, because he could see all of a sudden in the MAGIC summaries a flood of messages beginning about the Japanese military. Apparently, he had contacted General Corderman and General Corderman didn't want to get involved so then Bill Bundy contacted me. He said in the letter that he had contacted Corderman, Lewin was interested in a certain kind of information. What I did, I wrote a letter to the Agency. I sent it to Ann Caracristi, she was the Deputy Director, with a copy of the letter and said we had put in plenty of blood, sweat and tears, they kept this information, what do I do here? You see, I mean. So eventually I got a reply from the Agency which said they've been dealing with Lewin before apparently in some of his other books, and just tell Bill Bundy to tell Lewin to contact the chief of the historical section in the Agency, you know, and give him whatever information.

FARLEY: He came out, yes.

KULLBACK: I never knew whether he did. I thought so. I didn't know whether he followed up on it. But the interesting thing is I think he was trying to find information just about when a solution took place. This business of crossing of the information and I don't think he realized or appreciated the tremendous communications link we had between Arlington Hall and CB. Both exchanging the inflow traffic, so that I believe CB got a copy of every message we had. We had a copy of every message CB had, plus the exchange, but we got solutions. We relayed that information to CB. CB relayed their solutions to us, and the decodement. This is not evident from what he had access to, because these are only the MAGIC summaries which gives the output. So he could see that all of a sudden there's a period of time, there's a tremendous flow of information on the Japanese Army system. He mentions that. But he was trying to find out more and I guess he never was aware of, he may have known that there was such a thing as CB, but I guess didn't realize the close exchanges and everything that went on. So you know, he's looking at the surface of a tremendous iceberg, so to speak, and he really cannot see what is completely under that iceberg. That's why, when you read this, you know you get an impression the man really isn't aware of everything that he should be talking about. Where the devil is it?

FARLEY: How successful were we against all Japanese systems? I mean there were probably what, eight or ten different Japanese systems. How successful were we against each one?

KULLBACK: Completely

FARLEY: Really. Good!

KULLBACK: Completely. We were completely successful. As I say, by the time the war ended --the way we used to operate in Arlington Hall was, the IBM equipment had the codes on their cards, and there were two ways in which they operated. One where we developed an over-lap, in other words, were able to put together half

a dozen messages, four or five messages that fell on the same page, were enciphered by the same page of the key book. These would go down to the machine room and for these various columns, there were a list of the most frequent code words, numbers, I guess, unit names and stuff like that, which they would try of the various columns to start recovering the key if it was a page on which we didn't know the key. If it was a page on which the key had already been recovered, then they would apply the key, convert it to the basic underlying code and then, in effect, set up for each of these things a translation. In other words, the code word – its meaning, code word its meaning, code word, meaning. Then the translators would get these and then summarize the messages, whatever information and then it would go on to the intelligence people and they would extract from it whatever information they needed for battle order information, where the units were, the state of how many people they had, how many were sick, the state of their supplies, all of this business. And by the end of the war we were working in Wing 8, I think it was, of the Arlington Hall Station. One side of that wing, that was a fairly long wing – one side of that wing was stacked with IBM decodes from the floor practically up to the ceiling. These were messages that the translators and intelligence people hadn't been able to get around to because to a certain extent the translators and intelligence people would look over the various messages to pick out what they felt were the important ones or which gave clues to things that they were interested in. And, as I say, stacks from one end of the wing to the other. So the statement I made is we got to be so familiar with the Japanese communications systems that any set of messages which came in or which, if they were the captured books, for example. There was a radio intelligence code book which was captured. This was used very infrequently because it was only used by the communications people and they didn't do much trafficking. But we knew so

much about it that if we would get any of these captured fragments we could relate it to messages so that, I would say that, so far as the Japanese Army the high-level systems were concerned - we read them all completely. There were no gaps and, of course, because it was a code system, this is something some of these people don't understand, because it was a code system you could get in messages which, unfortunately, let's say, fell on a page of the key book that you hadn't recovered yet. You couldn't do much with it and you had to wait. First you get a reasonable number of messages to line up and then solve them. So that the guy like Lewin who really wasn't in the business, but got into it afterwards, he thinks in terms of the German Enigma. Sure, once you got one bit of information for the day the keying system, you could read all of the German messages in that set-up for the day. But you could get a lot of information about some of the messages in an enciphered code system and then no information about other messages depending upon where they fell in the key book. A lot of these people don't seem to realize that. And, of course, one thing which we got some feedback. Because people are always concerned about security, both of any operations that were being planned. But we would get requests from the intelligence people like , for example, Alfred Friendly. When they were planning some major moves against the Japanese, either against some of the islands or the last big move that they were planning was, of course, the invasion of the Japanese mainland. They would come and ask us, if possible, to concentrate on messages from or to certain places because these were the places which would be heavily involved, let's say, in any invasion or attack which was being planned, and they wanted to know as much as possible about the set-up of the Japanese fortification, their strength, and so on. And then what we tried to do in those cases was go through and select those overlaps which contained messages involving those places that they had asked us about. And I guess we couldn't

always satisfy their requests because occasionally a message that they might be interested in would fall either on a page for which we had no key yet or would only fall on a page which it was the only message. Unless there were some depth there wasn't much you could do in the way of solutions. But in the main, I think we were able to comply. And this is really how we assign priority to the work that was being done. Picture Arlington Hall, well, you've been to Arlington Hall Station. You saw those wings – we had rows and rows of tables, people working away like an assembly line.

TAPE V, SIDE B

KULLBACK: And it was quite an assembly line, and if there were no specific requests for a group of messages which said, "Well, work on this." You know the priorities that we assign. Then in the main, I guess, if we had more overlaps than people working them at the time, you take the deeper one first. They were easier to work on, do it that way, but after a while once we began attacking the Japanese and going in and the plans were made now that this is where we're going to invade and so on and get as much information as possible about those places. We had priorities about which overlaps – I presume the same things was done – I never really did talk too much with Sinkov, but I guess from what I've heard, Swears was there for a while. Apparently the set-up in CB was exactly, except that I think we had more people working in Arlington Hall than you had in your military units, plus we probably had a bigger IBM set-up. We apparently had a bigger IBM set-up.

FARLEY: We had about three machines, I guess.

KULLBACK: No, we had a fairly big IBM set-up. There was no question. But again, it wasn't a sort of machine set-up that you could ship overseas and then move it along as CB

moved to different places from time to time. And I think that the IBM people that we had, plus I mean the cooperation that we got from the IBM Company itself that built a lot of special machines for us, plus the ingenuity of the IBM people who we had in our machine section. Dunwell is one, Ed Dunwell in particular. So that in a number of times, when we got some, for example, the Japanese codes used to have the numerical groups. They just didn't assign the code groups for numbers in a random fashion, they assigned the code groups so that there'd be a self-checking scheme in it so that in a literal system we would have permutation tables so that if there was a garble you could at least reduce it to five possible groups if there was a garble. And since the Japanese were using all 10,000 groups in their code books, if there was a garble, it would be really difficult to know that it was a garble except maybe you're having trouble, the message wouldn't make too much sense. But in order to protect themselves against such contingencies all of the groups which represented numbers, I think they ran from one up to a hundred and a thousand, stuff like that, had internal self-checking features.

FARLEY: Sum checks?

KULLBACK: Yeah, sum checks so that if it was supposed to be a number, the Japanese operators, the code clerks, had a check on what that number would be. Now later on when a number of the Japanese units were being isolated on these islands MacArthur would by-pass them and there they were and the only way they could get some supplies was occasionally by submarine, in which some of them got through and some of the didn't. When they had to make changes in the communications system, this is one thing. The Japanese kept all these isolated units fully informed of what was going on, instead of saying, "Well, there isn't much you can do about it, you're isolated," but they really kept them informed and so they had to get to them key books, code books, and so on. And

the only way they had sometimes was to, for example, towards the end the enciphering squares which changed every five days, they could distribute them to a lot of places, but to some of these isolated places, they couldn't distribute them. So what they would do, they would send them, in effect, a message which consisted of ten digits – I mean, no – ten groups, because there are ten digits in a square, so ten code groups, ten code groups ten code groups, ten code. And these we could recognize that this was probably a message which was sending the enciphering square to an isolated unit. And because of the underlying pattern of the code groups the IBM people, first we told them what the problem was, and they came up with a possible design, and then the IBM Company built for us special machines and we used to feed these possible messages through this machine and every once in a while we'd get a hit and sure enough out would come the new enciphering square. We didn't have to try to recover it because for a while trying to recover the enciphering square we tried to do it by frequency counts. The digits. It wasn't an easy job. As a matter of fact, some of the statistical consulting groups that were available to us because they were doing special consulting for the Army in mathematical problems, Sam Wilkes, for example, who ultimately was the chairman of our Scientific Advisory Board until he did, was one of these men who were involved in doing statistical advice and worked for the Army. He had clearance, and he came to Arlington Hall Station to see if there were any problems that were such, you know, that these mathematical people could work on. And one of the problems we gave him was this business of seeing if you couldn't reconstruct these enciphering squares on the basis of the frequencies. Well, unfortunately, there wasn't that much variation in the frequencies so we really couldn't do much. But they gave up, it was a difficult problem. So that consequently being able to spot these messages, and it was done by a machine to recognize and get these enciphering squares

because towards the end I think they were, either they were changing the enciphering square every five days or maybe towards the end they got it down to changing it every day. You know, they were beginning to get more and more concerned about the security of their system, plus they had so many isolated units that they couldn't distribute this information so that they were sending them these messages. That was a big help to us. It was to CB, also, of course. I remember on one occasion they wanted to change the key book, 500 page book with squares you know, ten four-digit groups across the row, with scrambled up numbers on the side. In principle it was a fairly good system, but if you had a lot of volume of traffic then it would break down. And at one time they were going to change the key book, but they had difficulties in distributing it, and, so again, because we were reading all the traffic, what they were told to do was add, oh, that's right – what they were told to do was to compile out of their existing key book, a new key book by adding; for example, if you took the page one and page two, you added the digits, and you would get a new page one, then they take page two and three and add the digits and get a new page two. And go through the key book, do it that way, so it would end up, in effect, a new key book and if nobody knew what the old key book was, it would, in effect, be a problem of solving it all over again. But, again, fortunately we had the old key book, we read what they were doing, so we were able to compile, so when they changed the key book, there was no problem in being able to do that. As I say, once we got in the Japanese tried all kinds of tricks to maintain the security.

FARLEY: Did it get so complicated that it was extremely difficult for a Japanese cryptclerk to decipher a message?

KULLBACK: No. It got so complicated that it was difficult for our people if we had to do by hand what the Japanese Army was accomplishing. But fortunately we didn't have to do it by hand and we were highly mechanized. But their communication

systems didn't break down. I mean, I was always amazed at how they were able to communicate and the volume that they communicated, a tremendous volume of traffic, but using such sort of an involved system with the address book and its own key book and enciphering the address, and enciphering the indicator which gave the page, row, and column by its own key book separate and then the enciphering the text of the code messages by another key book. And also using instead of just the normal arithmetic so an operator could really do that very rapidly, you sit down and do it very rapidly, a scheme where, in effect, they were enciphering. They had to have this little 10 x 10 square and if it -- let's see -- yeah, it was an enciphering square. They used a row to represent -- what the hell, how was it? Oh, that's right. If you had the cipher digits -- how the devil did these damned little -- it was really the equivalent of ten alphabets to encipher so that when you enciphered it what you would have would be the plain digits and the key digits. That's right. You had a plain digit and the cipher -- no, no. You had what was your plain and the key, then you'd look up in the square, you'd look up the plain down one coordinate and then key down the other coordinate and where they intersected would have been the cipher digits which is the thing which was transmitted. Then the receiving clerk would have the cipher message so he'd have the cipher digits, then he also knew what page and row and column the key was taken from. He would then have the necessary key digits, so, again, what he would take would be the coordinate corresponding to the key and go down that column until he came to the cipher digit and then it would give him the corresponding plain digit. Now obviously that's slow. That's not as fast as the case when you write out the key and when you're using plain addition you just go and add the numbers. And yet in spite of all of that complexity, I say I remember when we used to have visitors, I would have to give them a picture of the Japanese Army systems, the progress.

Incidentally, we designated all the various changes in these systems by colors. Frank Lewis was the one who came up with what the color should be. I guess CB used the same colors, because we were exchanging, but I never heard some of the colors which – puce, magenta. I remember there was a puce and a magenta and a lilac. We didn't use purple and a lilac and others to designate. We had great big charts which we had prepared from the different systems, like for 2,4,6,8 over the various periods when the code book changed, when the key book changed and this was our lilac period, our magenta, puce systems and so on. I used to explain, go over that with them and then they had a table on which you had piled a copy of all of the books which the Japanese code clerk in one of the units had to have access to, like the address book and the key books and the code book itself and its key book and the address squares. It was a pile of stuff and I used to say that I didn't think the American Army would have been able to maintain a tremendous exchange of communications which were necessary in the way the Japanese did. Of course, our aim had always been mechanize, convert everything to machines, and so on. But so far as we could tell, the Japanese communications system never broke down because of the volume of material that they had to encode and encipher. And I don't think their cryptographic staffs were that tremendous that you could say, well, if you put enough people at it, it's something you'll be able to do.

FARLEY; Were they pretty security conscious, too? Or were they human and they did make mistakes?

KULLBACK: Well, they were security conscious and I think I mentioned to you the other time. If that document could ever be located again wherever the files are, if it hadn't been destroyed, when the war ended, we, still have a fairly large group of people, and the problem was now to convert from the wartime tasks, the Jap Army, to peacetime, reallocate the people. There were a number of tasks which

we did just to keep people going. The machines and so on. I remember one task, as a matter of fact, I have a book here which was a result of that. (looking for the book now). It was issued by the Bureau of Standards, Department of Commerce. But the manuscript (found the book, now looking in it).

FARLEY: Limited distribution. Mimeograph form by a branch of the Department of the Army just after the close of World War II.

KULLBACK: Now this was done. Well, first we were interested in the statistical kind of a table in connection with the cryptanalytic activity. We had the machine set-up and the work flow had fallen down, we had something to do to keep them busy, so we had to compile all these tables. And then we had them in the Young Security Agency in a soft mimeographed form. Then eventually we started dealing with the Bureau of Standards. The Bureau of Standards got involved in developing computers and I don't know, somehow or other we asked them if they were interested in publishing these things. I mean, because it's really nothing but a standard statistical table. We took a special distribution, and we computed all of the values of that binomial formula. We were interested in it because of its potential use in cryptanalytic activities. We had the machines available because we hadn't converted yet to new jobs other than the Japanese Army so we used this as a means of keeping people busy. Then the other thing which was done was, we had kept very close tabs, I told you, in the cryptanalytic section, Bill Erskine, on the distribution of the Japanese material to various units and also their messages, serial numbers, and so on, and captured materials and all of that. He was the head of a small group. So that we had a pretty good picture and if anyone of the people on the overlap wanted some advice or information about possible serial numbers, it was there. And so at the end of the war, tasks were done and we asked ourselves the same question. Here was a Japanese, you know, obviously they were security conscious. They had a

cryptographic section, they had quite a set-up with codes and so on. Just wherein did their security break down. We felt, for example, with the use of, at least on high level systems, the Sigaba, that we could tell, let's say from reading their material, that there was no indication in any of their communications that they were having success with the American systems. Towards the end they did have some success, but this was when the Air Force started taking off from the outlying islands to bomb the Japanese mainland and some of the closer islands. The Air Force apparently wasn't too security conscious and they would talk in the clear, so that the Japanese could try to guess what parts of Japan were going to be bombed. There wasn't much they could really do about it, because by that time the Japanese Air Force had been pretty well depleted, so that even if they knew where the squadrons, the attacks, American air squadrons were flying, there wasn't an awful lot they could do about it. But nevertheless they were able to pick up a lot of information from the chitty chatter of the pilot and so on. Also, I think they had captured some of the Hagelin machines and were able to read some of the low-level Hagelin, because the Hagelin traffic was used below division. They had very little success cryptanalytically with our traffic. Whatever information they would get you might say from direction finding, traffic analysis. We had complete success with theirs, and so you know, the question was, what were the weakness? And this is very interesting study which Bill Erskine wrote up. I think it's something which maybe the security people should have in their files. Really the question was, how do you draw a line between the extreme severity which the Japanese would apply to any outfit which was responsible for the loss of a code book or a key book and you know you can't pat the guy on the back and say, "Too bad!" I mean, there has to be some kind of a reasonable line between -- Now you see in the Japanese case, if a clerk lost his code book, he was supposed to report it. It would go up the line and the

consequence is he would be punished, his superior, everybody along the line. I don't know how high up they would go. It would be, you know, a relatively severe punishment. As a result, you see, the tendency was, if possible, not to report the loss of these documents, registered publications, and this. And their scheme was, when the code book, for example, went out of effect, they were supposed to tear the covers off and mail the covers back in as a proof and then destroy completely the book by burning it and mixing up the ashes and all that sort of thing. And I think I mentioned the other times, there were many instances in which we had a message in which the code clerk or the sergeant in charge of it, described very precisely the location of where he dug the hole on the each and the fire and the ashes and mixing up the ashes with the sand, and so on, and burying the book. And we had the book in our hands. It had been captured, gotten in some way. So that was one weakness in their security. The other weakness, well, but then, we also suffered sometimes when they thought that a ship which had been sunk which had a courier on board that we were able to recover the material which the courier was carrying. Some cases it did happen, and in other cases it didn't happen. So there were instances when they thought we had gotten something and we didn't, they made changes in it and there were other cases in which they weren't aware of the fact that we had gotten the material and didn't make the changes, so I don't know, it sort of balanced out. I think the other conclusion, with respect to security, was that they were so tough if there was a loss of a book or key, that it mitigated against reporting these things so it was very possible in a big military system for material to be lost, strayed or stolen without it being reported as such, because the people involved just didn't want to suffer the harsh penalties which would be a consequence of it. Then the other difficulties that they ran into were, you know, the usual ones which happen in this kind of a cryptographic system. You make a

change, or even actually with which happen with the German machines. I mean, a change is due on a certain day and somebody gets confused and doesn't make the change and then the recipient trying to read the message according to the new set-up or new something, can't read it. So he asks for a repeat and the guy realizes what had happened, so he takes

[REDACTED]

Things like that. But, also, I don't know, I guess it's also the sheer volume of traffic which was being sent which couldn't stand up under an additive system, with, let's say, with only 500 pages of the key book. In other words, you send these high-level messages in tremendous volume, you get enough depth and then once we knew how to assign these things to the right pages you could always solve a system like that. Takes just a little effort, but you know, one you got a reasonable depth you can solve it. So it was also inherent in the nature of the cryptographic system itself and with a system like that in a big military organization you can't change too often, because you then have the problem of distributing the keys to everybody (and they were widely separated) plus the problem of actually making them, getting reasonably random arrangements, publishing these books and all this. It's a tremendous enterprise. So that the system sort of, you might say, collapsed of its own weight. It's a system which would be fairly secure by an organization which didn't have too much into communication, so that one you'd be able to change the key books not too frequently, so just the sheer problem of compiling and printing these things becomes quite a burden. And also, over a period of time the usage over the key book itself wouldn't be so heavily concentrated that you can begin to get into it. The Germans ran into that same problem with their diplomatic system when they began to be in a position where it wasn't easy for them to send new key books. Like to South America. They were blocked, one thing or another so they had the same problem to a certain extent that the

Japanese had, where the same type of system under wartime usage, whereas with a machine system if you have enough rotors out to make a choice amongst the rotors, your problem is to devise a good secure system for indicating where the messages start so you don't have that tremendous production requirement. So it's quite true. C Branch, where they were making rotors during the war, was a pretty busy place, wiring up rotors, collecting them into sets of the machines and sending them out, make changes often. Sometimes it's the mere physical problem of trying to keep up with all the requirements. The Japanese, well, they were security conscious, but they were so convinced, I guess, in the security of their systems just, I guess, like they were in the security of Purple and all that business, that when things happened which could be possibly ascribed as the fact that the traffic was being read, they looked for other answers, for other solutions. And, these things, I don't know how true they are, but there are stories in these books nowadays which indicate that the Japanese were told that the Americans were able to read their Purple system, and they couldn't believe it. The Germans didn't believe, I guess, that the Allies were able to read their traffic, diplomatic, Enigma, and as I say the Japanese always suspected that spies and agents and secret things of that sort were the reason why a lot of the shipping was being lost and didn't feel that it was because of the fact that their cryptographic systems were being solved. For one thing, I guess, it would've implied a tremendous loss of face by the people who were responsible for setting up these things, and, of course, they wouldn't admit. Were you aware of the fact that the Japanese had worked on trying to devise a rotor type machine, ultimately if they were successful which would have replaced a lot of these hand code book systems?

FARLEY: No.

KULLBACK: Well, such a device was captured.

FARLEY: Based on the Enigma? Or based on what?

KULLBACK: Well, it was a takeoff from the Enigma or the rotor machines. And we weren't sure if and when they would actually ever get enough of these devices to replace the code books. But we had a group who studied the machines, the construction was very delicate, very fine wiring, and I think some of our machine people, I think Leo Rosen, for example, saw these and their conclusion was that the thing -- this was now after we had had experience now with the Sigaba in the field and all of the headaches that we had gone through with the Navy in getting the thing manufactured and broken in and trying to make it fool-proof and reliable, that the Japanese would have a lot of trouble in actually getting the machine to stand up under wear. And then also, the machine had -- the output was such that if they ever used it it would be recognizable as this machine I think the literal and the frequencies and so on. And we had arrived at potential ways of solving it and so on, so we were sort of trying to be prepared to tackle that traffic if it ever turned up, but it never turned up.

FARLEY: Was this fairly late in the war?

KULLBACK: Yes, this was towards the end of the war, yeah. And I guess maybe they had a couple of devices out in the field for testing purposes, and things of that kind. But, as I say, the machine people felt that the construction was such that if this was the way they were going to build a machine, they would be running into a lot of just maintenance, physical problems. And we had what we thought was a means of tackling it. Now, again, all of that is in the file someplace. I don't know, I'm just, I'm sorry I didn't keep a -- but I made no notes in this book, so that if anybody were to pick up this book, they wouldn't get any information from me about it. Where he talks about -- oh, by the way, here it is (looking in a book). This famous scroll we prepared which I presented to Mr. Friedman. that's

me (showing Mr. Farley his own picture). Where the devil is it? (flipping through the book).

FARLEY: You mentioned Enigma. Let me ask just a quick question that I happened to think of. There were rumors that the Coast Guard broke the Enigma shortly after the British broke the Enigma. Do you have any information on that?

KULLBACK: Our Coast Guard?

FARLEY: Yes. Mrs. Friedman's group.

KULLBACK: During the war they were incorporated into the Navy.

FARLEY: So you don't know anything about whether they worked on the Enigma at all or whether they had any success or whether they were even trying?

KULLBACK: A Coast Guard unit as such? On a German Enigma?

FARLEY: Yes, Sir, right.

KULLBACK: Well, which Enigma? Would it be the commercial Enigma or the military Enigma? If it was a commercial Enigma I can understand that, maybe there were some transmissions using the commercial Enigma for traffic which the Coast Guard would have been interested in, but the Coast Guard wouldn't have been working on the military or the naval traffic, and if it was at all during the war, the Coast Guard became an integral part of the Navy and so it would have been the Navy. They may have had messages like some of these agent messages which used the commercial Enigma and probably had success with it yes, but it would have been the commercial Enigma. And the commercial Enigma, well, we actually had a machine that, I think, the wiring in the rotors because in the commercial Enigma, I don't think they went to the extremes of changing rotors and so on that the military did, so it's quite likely, yes.

TAPE VI, SIDE A

KULLBACK: See, fortunately this courier was not an official diplomat, so he didn't have diplomatic immunity. This was an indication of some of the cooperation we really got from the FBI. Because what happened was the ship, I think stopped in New York and they went through their baggage because there was a war in Europe and this was I guess normal then for the FBI, the United States, to go through various ships that were going on to check, make sure that theoretically no contraband, whatever it was. The FBI spotted that this guy was carrying obviously some diplomatic material, because he was carrying a bag, I think, which theoretically had the seal on it and the German government, you know, like a diplomat would carry. But he didn't have the diplomatic immunity. I don't know what story they gave, but they took the material for safekeeping they said whatever it was, then they very carefully took the seal off because when they gave it back to him it looked as though it had not been opened, the seal was still intact and everything, and it did happen to contain one – a new code book which was being sent for the German diplomatic system. And also some keys to be used in the future. By that time we had a pretty good idea as to how that system worked – the double additive system, so we, when we got these keys and things, we knew exactly what they were, what they represented. Now apparently even though the material was resealed with the same German diplomatic seal and everything, I guess when it was reported that it had been out of his possession for awhile, the Germans did what any good security COMSEC outfit would do assume that the stuff had been tampered with. So they used the material, but not without instructing, we didn't know, as though we hadn't gotten into reading this activity, how to make changes in the encoding, let's say, by adding columns and stuff like that. But at least knowing what they had started with in the encipherment, we were able – well, first of all we got the code book which was a tremendous help for us, then you didn't have to try to

reconstruct this 50,000 - 60,000 word code book. And so that if we had some depth which we did get because laziness on the part of the some of the code clerks who had, they were too lazy to open the code, the key book at random and really use the theory, the instructions they had were to try to distribute their messages at random uniformly over all of the pages of the key book. Well, they didn't do that. Some of them had favorite pages or they had key which they had prepared in advance, you know, by writing out the additive and then another line or just shifting it over. They were just lazy, doing it the easy way. So we could start getting into some of the keys and key books and eventually found out what they had done to the daily keys which had been captured. In other words, the scheme that they had was, they would start out with two lines, which they added - they'd put them down - then they would add to these, the daily keys which changed, and then they would replace the digits by a consonant vowel pair group. That was more, I guess, for communication purposes, really it didn't involve any security. But we were able then to find out what they had done to use the basic material but what changes they had made. So it gave us a start and we had the code book which was a tremendous help, of course. Plus the fact that after we had gotten into the system and the British had stopped even intercepting messages, they had given up on the thing. This is where ignorance is bliss because we really didn't know fully what the problem was, what we were working at initially, and so we plugged away and struggled with it. Whereas it's quite reasonable to say that if you have an organization and they were at war, and facilities are limited and sources, funds are limited, and you have to try to put your effort on what will at least give you the most return. In theory, this double additive system was a fairly difficult one. They could see it was a difficult problem and they would have to put a lot of resources on it, whereas resources were scarce. So they used those resources on something for

which it was a better chance of getting a return. But actually they also had in their files what at the time they didn't realize what it was. But apparently one of their agents had access to the key book in some German embassy, like Asia. He had had enough time to copy out by hand the first twenty-five lines of that key book. The key book I think had five digit groups across on a line, I think there were ten to a line, and there were, I don't know, either ten, fifteen or twenty lines on a page, and these pages were numbered. He had enough time to copy that out. And, of course, the first keys that we recovered simply from superimposition(?). We got depth from Buenos Aires, fell on that first page, because that guy was lazy. When we recovered the keys what we recovered was not necessarily the original additive but like when you start on recovering the keys in the key book you don't get the absolute basis, you get relative basis, then you convert it to an absolute basis. And then once we were able to decipher some of the indicator lines, and know that he was using, let's say, the first twenty-five lines, also fortunately the lines that he had combined were from those first twenty-five lines. He was that lazy, he just opened the book to the first page and did everything on that first page. So the key that we recovered which was a double additive, once we assumed which lines were being used, we could split it apart and so we moved what we had there and thereafter. It helped a good deal because everytime the double additive involved one of those first twenty-five lines we could subtract twenty-five lines from it and reduce it to a problem of solving for just one additive. This is really how we began to reconstruct the key book, but starting where we could have one known line with one unknown line, and then subtract the known line and therefore recover the additive, gradually build up the book that way. It took quite a while, a lot of traffic and we were using all kinds of tricks where, let's see, some of the tricks. Where we had

recovered an additive (his telephone rings and he stops talking; returns after telephone interruption and Mr. Farley refreshes his memory).

FARLEY: We were talking about the courier and the...

KULLBACK: Yeah, but also when we were working on the reconstructing of the keys what we could do was construct, for example, if they used the line A and B, and the line B and C, and we recovered the combination of A and B, and the combination of B and C, then we could subtract those two lines and get rid of the B and, in effect, have a key which was A minus C. Now you see the way the key book was constructed, the first 5,000 key elements. It was a 10,000 key element book, where the complement of the last five so that, theoretically, the way they worked it the encoding operator would add the two lines which he specified and then the decoding operator would take the lines with the change of the first digit by five and take the lines down and add – so they always added. They didn't have to add in one case, subtract in the other case because the key for line one and the key for line 501 were the numerical complements of one another, so if you added one of these lines to the code then if you added the other line automatically you would get back – so this saved them from adding and subtracting so that in effect they made the problem simpler for us because it really wasn't to try to reconstruct 10,000 lines. We really had to reconstruct only 5,000 lines and automatically we had the complement. So, for example, if we had A and B, and B and C, and we subtracted and we got A minus C, that would have been the same as A plus the complement of C, so if that line were ever used, we already had the key. So that way we were able to compile and have additive keys available if they were ever used. Now initially because of the bad habits of the German code clerks, they tended to concentrate on certain preferred lines and pages I imagine their books were probably dog-eared at the beginning, and the back part untouched, so that we were able to build up the first part of the

key book, because there was a tremendous usage of them. We had enough volume on them. After a while I guess the security of COMSEC security office in Berlin -- what was the guy's name? I ought to remember it because he used to sign all messages which had to do with the system when they were changing and sending keys later on, so we were always on the hunt for messages with his signature, because we knew they would contain cryptographic information. And then I guess they got worried because they began to realize that there was a heavy concentration and usage on second preferred lines. They then began to insist from Berlin, the kind of instructions which said that if you use line A, B, C, D, one way, then for the other you have to use the line in reverse order, which at that time was fine for us because it meant we began to get more usage of lines which by the old system would have been used infrequently. So this was essentially what enabled us to reconstruct the entire 10,000 groups of additives rather than have a heavy concentration on certain favored lines. Then messages would come in and we wouldn't be able to read those because we hadn't had enough material to read the. So they did it at the perfect time so far as we were concerned and, as I say, later on then, too, when they ran into the same problem that the Japanese did, they couldn't send couriers out, and they couldn't get daily keying information to isolated places or where they couldn't get by ship or by airplane or by submarine. They started sending them the daily keying information enciphered in the messages. And this is where we could recognize those messages because they had the signature -- what the hell was his name? He was the head of the code security, the code compilation officer, and so that was a tremendous help. But it's the old story that once you get into a cryptographic system, particularly in wartime, with a large organization where some of their units then tend to become difficult to reach by normal courier means and they want to keep them informed, if they start using the system itself,

that same system that you're reading, to send them keying information and stuff like that, once you've gotten in they'll never shake you loose. Now the Germans tried all kinds of things later on with respect to their keys, transposing digits and all kinds of stuff, but once we got in they couldn't shake us loose. Also, it was very interesting. I was in England at the time working with the German code. This is where I first went there. They were over in London, whereas all the other activities had moved out to Bletchley Park, the military and naval.

This was a revelation. It was

interesting. See all these little things have now in the normal course of events when you got a piece like that you could file it and it relates to this, but unless you were working with the system, it wouldn't mean much. It wouldn't mean anything to you. And the same was true with the Japanese. We got so familiar with the Japanese traffic and who was sending what, that any material which related to one another, we could relate and if that one was captured we had the information. We were able to do a lot more than if this information had come to us but we didn't have a complete picture of what the Japanese systems were and how this fitted into the whole picture. So, of course, the more you know about your enemy's cryptographic system, the better off you are.

FARLEY: Were the Germans ever desperate enough to change the basic code book for their diplomatic system for instance?

KULLBACK: No, no. They never made any attempt to change their basic code book. For one thing, it would have been a very difficult distributional task for them to get copies in everybody's hands. So what they did was try to make changes improving the security of the encipherment system. In other words, I suppose they came to the conclusion that the security was not inherent in the code book but in the cryptographic system which we used to encipher it. And so they went to all sorts of pains to, by regulation, force a flatter use of all of the keys which would have been fine, and if they had done that initially it would have made our job much more difficult, but unfortunately for them they did it too late and fortunately for us it gave us access. More access to lines that otherwise we wouldn't have had much usage on because of the favoritism shown by the German operators, plus transposing instead of copying the digits in the order 1,2,3,4,5, rearranging the order of the digits and things of that sort. But that really didn't accomplish too much because we were in with them. These are some of the difficulties that I suppose any large outfit, whether it be military, naval, diplomatic has to take into consideration in assessing the security of their own systems. I mean, these are things which lead to breakdown in the security. But the Germans, the Japanese really seemed to be much more physical security conscious than they were cryptographic security conscious which was to our big advantage. So what difference does it make if the cryptographic activity had carried on in a room without windows in which you can only get through from a trap door in the room below, if the nature of the cryptographic system you use doesn't permit much security. You've got physical security, fine, but from the point of view of an alert cryptanalytic enemy they're concerned more with the cryptographic security rather than the physical security in the office which does it.

FARLEY: Were the Germans aware or were they pretty confident that their systems were "secure"?

KULLBACK: Yes, I told you, they were in it to change and particularly with Buenos Aires, in which they accused Buenos Aires of laxity, one thing or another. They were really lax and careless in the usage of the system, but the answer Buenos Aires sent back showed that they were thinking of cryptographic security, I mean physical security. And they gave us a description of how the code work was being carried on in the room, windows barred door with no access to it, the guard outside, the pistols on the table, the great big police dogs and all of that business, which may have been true, but in that room the code clerk down there really committed, from a cryptographic point of view, very serious violations of cryptographic security. He was really our "in" into the whole problem. If it weren't for him, if other places had been, or if he had been as careful in the general use of the system, it would've been a hell of a job getting into it.

FARLEY: Did you make any trips over to CB from Arlington Hall during World War II?

KULLBACK: No.

FARLEY: Aside from going to England, that's the only one?

KULLBACK: Slip Swears made a trip for us.

FARLEY: What was the purpose for sending Slip out there, to CB?

KULLBACK: Well, for one, I think was to show the flag and I think the other was the usual complaints because the people were thousands of miles from home and those who were married were away from their family. You know the usual gripes which an outfit would have if it were thousands of miles from home, working hard and apparently feeling it wasn't appreciated or whatever it was. And so this was to bring love and kisses from Arlington Hall, see how they were doing things, try to smooth any rough spots which might have existed in the sense that maybe CB thought they weren't getting everything from Arlington Hall that

they should be getting, and stuff like that. So it was more a liaison visit really; find out what they were doing and try to take care of any complaints which were reasonable complaints and with which we were at fault and to tell us about what their problems were. It was primarily just as I say, to exchange ideas, see on the spot what was going on, do what he could to alleviate them or make recommendations to alleviate them. That was the primary reason.

FARLEY: Did Jim Fuld replace him? He came out to Australia, I remember as a liaison type.

KULLBACK: Jim Fuld.

FARLEY: F,U,L,D.

KULLBACK: I know, I know. Jim Fuld, seems to me he may have been. I think maybe once Slip was out there, he may have made a recommendation that we should have sort of a liaison guy out there. Not a member of CB, but somebody from Washington, so to speak, to see what problems there were. If Washington was responsible to communicate these things back, maybe that was Slip's recommendation. I don't recall it. In fact, I don't even recall when Jim Fuld went out there, but I think Slip was the first one and it may have been that as a result of what we felt with the smoothing out of things which Slip was able to accomplish in his recommendations, that we then sent somebody after Fuld and possibly somebody after him.

FARLEY: But I remember reading many detailed comprehensive reports by Fuld back to your organization about what was going on at CB.

KULLBACK: That would be the nature of the responsibility of the liaison officer.

FARLEY: But they were pretty, as I say, pretty detailed.

KULLBACK: Now I know so far as we were concerned, B-2, our outfit, we forwarded to CB everything we had. We never kept anything back. I mean, once we cleared this business with General Corderman the links were set up in communication. Nobody checked or supervised what we were sending or the material we were

sending. We had unlimited access to a communication link or communication links, because I know there was a tremendous amount of material going and we were on-line I guess 24-hours a day sending stuff and receiving stuff. So from our point of view we were shoving everything into the pipeline that we could, but I guess at the other end, you know it's understandable that people would be unhappy, they were so far away. I guess the liaison officers with their reports about what was going and so on helped clarify a lot of problems, clarify a lot of things. So it was apparently a very useful function that they served.

FARLEY: Did you ever have a morale problem in your organization?

KULLBACK: Sure, I told you about those lectures by Alfred Friendly and...

FARLEY: But that was to improve...

KULLBACK: That was just primarily to improve morale. Here were all these girls and working odd hours, swing shifts and the night shifts, and social life was fairly limited because of the war. I think unfortunately, some of the recruiting officers may have lied a little bit in order to get these girls to come to work in Washington by maybe implying that there would be more younger officers available. So, of course, there were quite a number of marriages and so on which resulted from working together, but there were many, many more of these girls than men. And life wasn't too pleasant, I guess. The girls doubled up, they weren't getting tremendous salaries. It was quite -- now after a while all they could see was they were working hard with this pencil and paper pushing it. So what, they'd say. They couldn't see any results and especially if they worked the night shifts. Those who were rotated so as we give everybody an opportunity to enjoy the swing shift and the graveyard shift. These who volunteered for it there was no problem, but not everybody volunteered. We tried to rotate so people would have a shot at day shift and swing shift and graveyard shift. And so it was necessary to build up their morale and one way was to have people like Alfred

Friendly come in and indicate how their results were making a tremendous difference in the intelligence picture, and with battle order, and what would be planned. And, as I say, Frank Lewis and I used to spend many a night just walking around talking to the girls, working, sit down and working with them. Particularly the late night shifts just to show that not only the girls themselves were being asked to work the nightshift, but even head of the outfit, deputies, assistant would come and work nights. And there used to be parties and picnics and one thing or another. So it was a morale problem, too, but it was maybe a little easier to take care of it in Washington. Well, the reason for the morale problem, I guess, in Washington was somewhat different from in -- that how far away 10,000 miles -- in Australia in a military situation, but it was the same kind of a thing. It was sure definitely a morale problem. Now in the address section, that Wilma Berryman, Wilma Davis headed up, Ann Caracristi was her deputy, that's about when Ann Caracristi came into the Agency, and that outfit was 100 percent female. There were only girls working on that address system, reconstructing the address code and the keys and so on. The messages would pass first through the address unit, they would put the addresses on and then get on to the overlap so that ultimately the translation would include the address radio link and all the other information. And there were just officers assigned to that unit. And I don't know if you ever met Rueben Weiss, you may have. Rueben Weiss and Mort Barrow were the two officers who were assigned to that section which probably had at least 100 girls. Rube Weiss and Mort Barrow were my battery on the softball league. Rube Weiss was the pitcher, and Mort Barrow was the catcher. Did you get to know Joe Valentino? He was down in the shop there for a while. He was third baseman. I was center fielder. Boy, there was a lot of finagling going to to try to get people assigned to the different sections -- COMSEC of the PROD or the Japanese section according also

to their ability on these local teams. There was intense rivalry in Arlington Hall and it was again part of morale. This was again part of General Corderman's, I mean, as a military individual, I think he was aware of the need that the military people needed some form of athletic participation from the point of view of their own well-being and health plus as morale. And, of course, there was a period, I don't know if it was in those days, at least before the war, where all of the officers on duty in the Munitions Building, Wednesday afternoon were always off for athletic activities. So he as commanding general, you know, saw to it that these things were organized, competition. In fact, I got into bowling tenpins, we used to bowl duckpins. Where he got into bowling, of course, he was interested in tenpin bowling, he'd come from, I guess, around Ft. Monmouth where tenpins were the most popular form of bowling rather than duckpins which was initially the bowling in Washington. Now, of course, tenpins have taken over much more completely than duckpins, which still exist. And he set up, we used to bowl at night, just the Arlington Hall officers' leagues and so on. He was conscious of the need for physical exercise and recreation. In fact, also, we used to play basketball and, who was it, I think it was Joe Valentino. I'll never forget, was it he or Arnold Dumey, one of them, they were playing basketball and unfortunately he jumped up at the same time with Corderman for a ball, and when they came down he landed on Corderman's foot and sprained it pretty badly. I mean, you know, the junior officer having sprained the ankle of the commanding general of the outfit. He didn't know what was going to happen to him. But, as I say, all of these things, there were a lot of – morale and the address section with Mort Barrow and Rube Weiss was one of the little groups which had few morale problems because really, Rube Weiss was always a comedian. I don't know, somehow or other those two officers kept the spirits of the girls in that address section up high.

FARLEY: Mort was a good looking guy, too.

KULLBACK: That helped tremendously. But I remember particularly that section because there were only those two officers and a hundred girls or something like that. But they kept up the spirits of that group and again that was a group, too, which had to work three shifts because the operations went on day and night. And we had morale problems, yes, but they were solved in a variety of ways. The intelligence people would come and indicate how useful the material was. How it was being put to use. Particularly to those women, quite a number of women there were married to soldiers overseas and this meant a good deal. Plus Christmas parties, picnics, you name it we tried everything to keep the spirits up.

FARLEY: Was there friction between the military and the civilian? I'm thinking of the WACs and the civilian gals, envious of each other or worrying about pay scales?

KULLBACK: Well, I don't know, there may have been some. But we operated, the B-2 section, now some of the younger officers who'd just been out of Officer Training School, initially may have been a little bit put out, because they would be assigned to one of the units, Japanese military section, and lo and behold, who was their boss – a PFC or a sergeant. Now some of these PFCs were old time Agency civilians who eventually were drafted and inducted or sergeant who had been in that way. The people who were put in charge of a unit, it wasn't a question of what their rank was, it was always a question of their cryptanalytic knowledge – expertise. And so initially, some of these junior officers especially felt here they'd gone through OCS, I am a second lieutenant, and I have to report to a PFC or a sergeant. Those who were able to take the explanation and realize that even though this guy was a sergeant, he knew much more about what was going on than the lieutenant knew. The lieutenant had to learn from him. That was fine. Those who couldn't make the adjustment, who were so military

imbued that he's a second lieutenant, he doesn't take orders from a sergeant no matter what it is, we got rid of. Some of them ended up in CBI must admit.

FARLEY: Oh, is that right?

KULLBACK: Oh, yes, they would, we would, we had to provide quotas overseas.

FARLEY: I can think of two or three of them.

KULLBACK: Some would go to CBI and we had to provide them. These were the officers that we would recommend and shipped out there. Now it could very well be that once they got to CB and they were in the military organization, everything was military, they could make the adjustment. But some of them just couldn't make the adjustment breaking in an organization which was mixed civilians and so on, or some of them resented the fact that they were in a unit in which a civilian was in charge. I mean he was military training and all of this and all of a sudden he has to report to a civilian but, you see, we were a very funny outfit. And we didn't go by rank, we went by knowledge and expertise. And those who couldn't adjust to that, we gently, whenever we had occasion that we had to supply an officer for an overseas assignment or elsewhere, they were the ones who were nominated.

TAPE VI, SIDE B

KULLBACK: We had some who weren't really professional military. They had gone through and been trained, but they were so imbued maybe with what they'd learned that when they would come on duty, for example, if they would get an assignment on the swing shift, when they reported it was always as though it was a change of flag officers. Everybody reporting, taking command, you know, going through that sort of business. We had some like that. But they would make life very difficult in Arlington Hall in a sense, and even though it was

basically run by the military, it really wasn't a military organization as such. There were a lot of civilians there and some of the real people with expertise were civilians. And some of them who were enlisted men happened to have been some of the long-time civilians who were drafted and we'd got them back again. So, obviously, in a place like that you didn't go by rank, you went by what people knew, and if the second lieutenant knew more than the sergeant, he would be in charge of the outfit, but if the sergeant had more experience and expertise than the second lieutenant, he would be put in charge of it. The same thing was true in Bletchley when I was there in England for the three or four months. It was a mixed up unit, a mixture of military, naval, and civilians and very informal. They had no requirements there that the military must necessarily wear uniforms. Now at least at Arlington Hall everybody who was in the military service wore the appropriate uniform. That even in Bletchley the British didn't require that. Then they, too, had -- as a matter of fact, I don't know if you've heard this story before. But they tell a story of about two Air Force officers who had been wounded and were assigned to Bletchley to help with the air problems at least while they were convalescing. And somehow or other they got the idea when they got into Bletchley that it was a mental institution -- that they were being assigned to a mental institution. They went in, they reported, and if you looked around the place and at some of the people who were there and the way they dressed and all that business, you could well believe that it was a mental institution. Had some real characters who were the brainiest people in the world, but in appearance and everything else they looked like real characters. And the story is that these two officers looked at one another and said, "This is a looney bin, what are we doing here?" And so they turned around and walked outside the gate. Then they got outside the gate and they stopped to think for a minute and said, "If this is the looney bin then maybe it would have been easy to

get in but difficult to get out. If we got out so easy there must be something else.", so they went back in. Now, as a matter of fact, they tell stories of, what was his name? The famous mathematician.

FARLEY: Starts with T, letter T? He had tuberculosis?

KULLBACK: No, he didn't; committed suicide.

FARLEY: Oh, yeah. I was thinking of Tretner (Turing) or something like that.

KULLBACK: His name is connected with machines, such and such a machine.

FARLEY: I know of whom you speak, but I can't recall his name.

KULLBACK: All right. He was involved in some of the work with the bombes and the German Enigmas and this sort of thing. And he had been originally a well-known mathematician, a lot of them from Cambridge and Oxford, and he had done a lot of work even later on after the war, worked with the theory, concept of computers. And there is, they talk about certain computers with his name. In any case, all these people used to have to fill out a form about, what is it they would call it? Home guard, and air raid defenses and so on about information and whether they would participate and he said, "No." He wasn't interested and wouldn't do this and wouldn't do the other thing and nobody ever seemed to either read it and get upset about it or something, but they had quite a conglomeration. Now we had, too, at Arlington Hall Station quite a conglomeration. I think we could have staffed a first rate university from amongst the people who were assigned, both military and civilian, who were assigned to the Arlington Hall Station because we got a lot of university people who were inducted either as enlisted people or come in as civilians. A lot of them came in as military and given their direct commissions. And so between all of these, we could have staffed really a top rate university. But the grounds with the people on it didn't really look as motley as Bletchley did. But I think at least it was a little bit more formal. General Corderman as a West Point graduate and

a military man was a little bit more of a, I wouldn't say a terrible stickler, but he thought, you know, there were certain limits and particularly amongst the military. The wearing the uniform and this sort of thing. Of course, all the military people had to comply, not only with that, but we also fire and go down to the rifle range and go through the barbed wire, the infiltration course and occasionally he would hold a parade with the enlisted men and that sort of thing. So it wasn't quite as motley looking outfit as the British. As a matter of fact, Corderman also had a good sense of humor and this incident would definitely prove it. There used to be coke machines, the Army version of the coke machines, I guess. You put in a nickel and a cup would come and you would get a coke. Well, it wasn't long before the people discovered that the machine, when you dropped a coin in, would turn on. But if you pull the plug out, the mechanism which turned it off failed to operate. So people would go in there and put in their nickel and get a cup, pull the plug out and everybody in the wing would go get their cup of coke. So after a while, after a while, the vendor who filled these machines sort of looked at it and began to complain to General Corderman about the fact that here is a machine at the end of a day, all of the cokes and so on were used up and gone but he only finds a couple of nickels in it. "What gives?" I guess eventually Corderman checked and found out about the fact that people had found out that if you pull the plug once the machine got started then the mechanism which shut it off would fail. So he sent out a very cute notice to everybody in the Arlington Hall Station. It said, "Now that we have solved the machine and have enjoyed some of the fruits of that solution, I think we ought to provide the vendor with a nickel for each cup of coca cola."

FARLEY: That's great.

KULLBACK: Really, that was a very interesting reaction and the way he phrased it.

FARLEY: Solved the machine.

KULLBACK: Solved the machine, solved the machine. We've had our fun, the guy is entitled to his nickel for a coke – coca cola.

FARLEY: That's great.

KULLBACK: Let me see, I think there were a couple of other points on here (referring to the question sheet Mr. Farley issued to him at an earlier date).

FARLEY: We have just about exhausted World War II, haven't we?

KULLBACK: Well, this I talked about, the early use of the machine. That's our first borrowing of the IBM machines, and that Friedman was able to convince the Signal Corps to provide us with one each of the punch, computer, the sorter and the tabulator.

FARLEY: Yes.

KULLBACK: Any need to discuss anything more about the solution to the Red and Purple machines? Any unique information which is not now a matter of record? Well, the Red machine was a lot easier to solve because it was simply an expanded version of a Kryha type of machine. The only difference there was that it had two wheels, one for the consonants and one for the vowels and the twenty wheel and the sixth wheel. The Purple machine I guess is really a remarkable achievement even compared to the solution of the Enigma machine, in that the Purple machine was solved from scratch with no idea what the machine was like or anything. At least the Poles had captured a copy of the military machine and they had gotten some ideas which then the British were able to exploit and build into the bombes so at least it wasn't a solution from scratch. So I think the Purple was a greater achievement cryptanalytically than the solution of the Enigma. British had that very well organized. We'll discuss the matter of U.S. Army/U.S. Navy cooperation in the pre-Pearl Harbor days. There was cooperation, but it was really sub rosa because Mr. Friedman was on good terms with some of the cryptanalysts in the Navy. He would exchange information and we did work on the, their modified version of the Hebern machine as a security study for them.

But it wasn't really very open. I don't know it that was heavily encouraged by either the Army or the Navy. This is the impression you get.

FARLEY: This seems to come through with most people I've talked with.

KULLBACK: There was some, and as I understand it, the attitude of the Navy was that they didn't want to tell the Army people too much because the Army was practically all civilian. The Navy was practically all naval people, and so they didn't trust the security. I laugh about that every time I read these revelations and how many of the Navy people have been mentioned by name and what they tell and practically very few Army people ever turned up as having discussed things with these authors.

FARLEY: Contradict the Navy troops, for sure.

KULLBACK: Would you care to relive those old days? Well, there were exciting days, but as I say -- the "Winds Message." I was sort of on the outside looking in and we were aware of what was going on but we were busy with our own problems, except that you know the Japanese traffic was important. At least within the organization, we knew what was going on with the Japanese traffic, and so on.

FARLEY: You mentioned the "Teapot Dome" scandal communication some time ago in an interview I read.

KULLBACK: Oh. Well, of course, those things when we got to it were messages which Mr. Friedman gave us as part of our training program. They were code messages. The solution of those things had occurred years before and it turned out that the FBI, or whoever was investigating the Teapot Dome scandal at the time, had gotten a lot of messages which had been exchanged by some of the people involved and Mr. Friedman was asked apparently for many, many years, anytime any coded, ciphered, cryptic communication came into the hands of anybody in Washington, somehow or other they were all funnelled to us, down at the Washington office. It came to him and apparently he saw it was some kind of a

code, thought it might be a code which was commercially available or something, which is what it turned out to be. He found the code so he was able to read all of the messages for the investigators and I think that was partly responsible for whatever the trial and what was his name? Fall and all those things were indicted and sentenced. But by the time we came to Washington, this was past history and he gave us the code messages without the book and we were supposed to use that as the material to try our code solution practices on, training material. "Would you account it – comment on Jap Systems?" Well, the Japanese Army systems, they were all exploited. There wasn't a one which we didn't read.

FARLEY: Was there any such system that was really a Japanese Army or ground force system, or was it the administration, the Water Transport?

KULLBACK: Well, the Water, they were all Army systems, of course, the Water Transport System was the system used by the Army. Apparently the Japanese Army had its own Navy really, but these were all commercial vessels. So that was used by them. Then the administrative system was the Japanese Army high-level communication system between, I guess it leads down to division. Then the Air System was the equivalent used by the Japanese Air Force. And then they had some odds and ends of systems. They had a code book and the corresponding system which the communications people used. But they were all Japanese Army, high-level systems. Then, of course, what the CBI people had to confront were the lower-level. But the fact that they were lower-level didn't mean that they were easier cryptanalytically because they were code, enciphered codes and even though they were three digit codes or something like that, nevertheless the volume of traffic that they had wasn't sufficient that they could get a lot of overlaps and do an awful lot with. So far as the high-level systems were concerned, Japanese Army, I would say that every message that came through

Arlington Hall Station was read or necessarily translated because they had a limited number of translators and what was done was glance over a lot of these messages and pick out the important ones. Or if they were looking for information about battle order selecting those and the others would be available in the file, but they were all there. Well, we talked about some of these funny things. WW II. "Discuss your position to which you were assigned after the end of the war in the Pacific."

FARLEY: Have we covered enough from World War II? Do you want to pick up...?

KULLBACK: Well, let me see.

FARLEY: I was thinking maybe the end of the war, or see what else? I didn't give a complete list of questions there because I didn't know how much time we'd have.

KULLBACK: Oh, "Comments on Rowlett move [redacted]" I don't know, that was kinda interesting. General Canine, I think this was when the building in Ft. Meade was finished and we were moving out there, wanted to make some reorganization. Sinkov had been in charge of communication security, A. B. Clarke had died just about that time, and I had been, what'd they call it, Technical Advisor in the Army section. Rowlett was in PROD, cryptanalytic. And General Canine appointed me as head of R&D, didn't go outside the Agency then to bring in people, like Bell Lab people. He arranged to have Sinkov take care of the production, I mean as a change. And he appointed Rowlett to be head of the COMSEC. Well, apparently Rowlett didn't take to that idea very well. I guess he preferred working in the cryptanalytic side than in the C SEC side, so apparently he looked around and had whatever influence, if there was any influence that was necessary, and he transferred [redacted] And then he worked [redacted] five or six years and then when Canine was retired, he came back to NSA.

FARLEY: He didn't get along with Canine very well?

KULLBACK: Apparently, apparently he didn't. It isn't a matter of getting along. Canine was the Director of the Agency so you had to get along with him. But apparently he wasn't happy about this change to C SEC, so he had an opportunity  and he did that. Then when Canine left the Agency, he had an opportunity to come back so he came back to NSA and at that time he didn't go back into the the head of PROD. Then for many years he was, in effect, the kind of job that Friedman had which was a technical advisor to the Director of the Agency. Because that's the kind of job he had right until I think he retired. But apparently he didn't agree with, let's say, with all of Canine's thoughts about rearranging. "Discuss your position to which assigned after the end of the war in the Pacific." Well, it depends. Right after the war when ASA reorganized, I was appointed head of the new R&D branch which was good – developed. Rowlett was in the PROD, cryptanalytic, and Sinkov was put in charge of COMSEC activities. Then when we amalgamated with the Navy on the AFSA (Armed Forces Security Agency) a naval officer was put in charge of the R&D activities. That was Captain Harper and I was made a technical director. Then after General Canine came in and NSA was formed, I think General Canine tried to go outside the Agency and get some retired (he went to Bell Labs) and he brought in A. B. Clarke who had just retired as a vice president, technically, from the AT&T out of Bell Telephone Lab. I was still retained in the position of the technical advisor and then we moved out to Ft. Meade. When Clarke died very suddenly, apparently Canine offered me in, I mean he called me in, offered me the job as head of R&D for which I was grateful. So that was the sequence. I was head of R&D until I retired.

FARLEY: Do you remember in that time period the deputy director by the name of Joe Ream?

KULLBACK: Yes.

FARLEY: Can you tell me anything about him? Where did he come from, where did he go, why did he go, why was he in the shadow so long?

KULLBACK: Well, for a while there, also the Pentagon was trying to get into the control of NSA. Part of the reorganizations we went through, also included control, more control by the Pentagon of the administrative activity and Joe Ream came to us from the Penatagon, either directly or indirectly as a deputy director. But if I recall he didn't stay on an awful long time. Now, I don't know whether he had come in from the outside, I think he came in from the business world. He may have come in or whether he thought it was? -- whatever the reason, I know he didn't stay on too long. But it was always there, the problem of the chain of command, and I think eventually the Pentagon set up an assistant secretary who was responsible for supervising the budget, the activities of NSA. One I remember was, oh, what, his father was a famous mathematician, Italian...

FARLEY: I want to say Busch.

KULLBACK: They name integrals after him, some kind of? Fubini. He didn't come to NSA as a deputy director, he was in the Pentagon and I think our budget had to go through him, some of our activities. He had been, he had been a vice president or something in some company that was interested in essentially what you would call traffic analysis and manufacturing, equipments. But then, the Pentagon began to get more into the act and our budgets used to have to go through to the Penatagon for approval. They would cut and tell us how much, and how this and the other thing. So that, in effect, General Canine, at least the Director of the Agency, General Canine reported at least in that activity through this assistant secretary up in the chain of command. Obviously, well, I think General Canine, when the Agency was first established, had a difficult position in that he had a lot of bosses until they clarified really the relationship between NSA and the three services and who will exercise what control. Actually, I think,

if at the time NSA was formed, if the Director of NSA had not been a strong and sort of farseeing an individual as General Canine, we may have had to go through another reorganization. I mean the thing may have fallen down. I think the big proof that General Canine was a good Director of NSA at that time, and the relationship which existed, the Army was jealous, the Navy was jealous, the Air Force was jealous, because part of their responsibilities had been taken away by NSA and both with respect to their budgets involving cryptographic and cryptanalytic activities. The fact that nowadays when a Director of NSA reaches a point at which he is relieved of this NSA assignment, they make him Chief of Staff of the Air Force, or the Chief of Staff of the Army, they promote them, apparently they realize. Whereas, unfortunately when it was General Canine's time to leave NSA he had to retire. I think that represents a big difference which has developed subsequently in the relationship between NSA and the services. The fact that the Director of NSA, when his time is up is, in effect, promoted, becomes Chief of Staff of the Air Force or the Navy out in the Pacific, you know where that could be. Whereas, Canine, that would have been unthinkable, but I think the foundation was laid by General Canine so that these things were possible. We in R&D in those days were faced with a very funny responsibility. We had to prepare and operate and do the R&D activities of NSA. We also had responsibility, but no real authority. We had to go over the Navy R&D budget and if we tried to cut it they raised holy hell. I mean they made life miserable for us. The same was true with the Air Force because the Air Force then was trying to establish the Air Force Security Service and the Army maintained the Army Security Agency. Small was there. He was trying to not be swallowed up so to speak by NSA. So we had such a funny dual responsibility in R&D that when I retired, I don't know whether I made the recommendation or not. The R&D responsibilities were then split. The head of R&D was responsible for the

activities within R&D and then a group was set up and I think the first one in charge of that was Leo Rosen. And that group, in effect, was to overlook, oversee the R&D budget, the Army budget, and give them a little bit more authority. So instead of putting a double burden on the head of R&D to operate and be responsible for the R&D budget within NSA, and at the same time be responsible for passing on the budget of the services, which was a hell of a responsibility, particularly if you tried to cut ten dollars out of a budget of one of the services, they would raise hell. I mean you were ruining them by cutting the, and so. I don't know, it's twenty years since I've been back there, but I presume the Agency still has some kind of dual or at least another activity, which isn't responsible for running things in NSA, but responsible for seeing that things are the budget anyhow by NSA and the services. I mean to give the NSA people the responsibility for doing things and then also of controlling the service budget. Put the R&D people at NSA on the spot. At least this way they know this is their job to carry this out. Here's another group which is like the Pentagon type and they're responsible for trying to allocate reasonable amounts of the budget and things which have to be done, and approving what sort of projects should be worked on, and what sort of projects should be given a lower priority and all of that.

FARLEY: Who generates most of the projects within R&D, the analysts who have a requirement or a need for a certain type of equipment, or the engineer who wants to come up with some idea to help the analyst? Is that a weird question to ask?

KULLBACK: No. The R&D had its own cryptanalytic mathematical research group which kept in touch with the requirements in PROD. R&D also had a cryptographic equipment development section, and we had the research mathematical group which was also able to do security studies and ideas of that sort which kept in

touch with the C SEC people. The development of the cryptanalytic devices and some of the contracts for the equipment were carried through R&D but the ideas, the needs and the requirements generated by the problems that PROD was working on. Now, for example, a project like the HARVEST, which wasn't a specific cryptanalytic machine, but which was more in the nature of a large general purpose computer trying to get beyond the current state of the art and get into a system which could handle things with high-speed memory, rapid access, tremendous large capabilities. This was really a joint idea between the R&D research people and the people in PROD, who, let's say, having needs for certain kinds of capabilities. Then those needs and capabilities were essentially translated into requirements and we went, let's say, to IBM particularly. Dunwell had left the Agency and was down working in IBM.

TAPE VII, SIDE ONE

KULLBACK: And these needs so to speak presented them. In other words, we need a device which can do this, that and the other thing, operate at such speeds with these capabilities. Then the IBM people would have their research group of people work and come up with some ideas and there would be an exchange back and forth between the IBM people and the R&D people who, I guess, theoretically were supervising the contract. Plus the people in PROD, who were really to be the ultimate users of that kind of machine people in PROD, ultimate users of that sort of a project. And from this eventually developed this concept of HARVEST and there were a lot of things built into HARVEST which were beyond the state-of-the-art at the time, I think. In terms of ideas and machine operation, I think were some of the things that were in a program trying to anticipate a certain number of steps before something was to happen so that the machine was

ready. In other words, to keep the machine running fast, take advantage of the full speed, instead of reaching a point and saying, I have to do something now and getting the machine to rearrange and organized to do it. Anticipate the fact that in ten steps you'll want the machine to do something, so getting the machine prepared so when this thing came up the machine was ready to do it. Now that would save microseconds, but nevertheless you save enough microseconds and lo and behold you got a tremendously fast machine. And eventually these ideas back and forth between the IBM Ppeople, their contribution, and the design of the equipment to do these things and the R&D people who I presume were certainly responsible because it was an R&D contract, plus the contribution of the PROD people resulted in what was the HARVEST system, which I think was a tremendous step. And I think the IBM people for a while really didn't know what they had in the way of capabilities and techniques because I think Dunwell's contribution there was downplayed for a while in the IBM company until somebody there realized that they had here the basis for a new generation of IBM computers. I think they knew that they were then so proud of a new generation of IBM computers was to a large extent based on techniques and ideas which had been developed in this HARVEST project. It's quite true. Later on I think the IBM people recognized Dunwell's contribution and did some appropriate recognition of this partner thing. But originally apparently I think they thought they spent a lot of money at a dead end that they didn't see any commercial possibilities for it. Now what were we talking about. How would their projects be initiated. Then the same thing was also true on the CSEC, I mean. The people, our CSEC, our R&D people were developing mathematical techniques, particularly ideas about generating sequences of plus-minuses which were purely random. Even if you had a long string of them you shouldn't be able to reconstruct the mechanism which was

generating them. That was the important thing, of course. Because so much of the communications was going over into digitalizing whatever it was you had, whether it was speech, or pictures, or ordinary teletype. Everything the input would be a stream of plus-minuses and the encipherment would be to add these random plus-minuses. and problems there was how you avoid depths because if you had the same key used in strings of these things, you line them up and it's not too difficult a problem. Because it's actually just an alphabet with two symbols. So the random generation of these things was how to avoid depths. Then also requirements which came in from the services. For example, the Navy, I remember, we had a requirement that a communication system so that after all they communicate in different time zones all over the world and particularly with submarines which may come up at night and they want to communicate with them, not necessarily have the sub communicate back because, the idea, I guess, is that ships should maintain silence to prevent their detection by radio direction finding, but they have to receive these broadcast messages. The problem the Navy had about messages which were intended, let's say, for battleships but not for destroyers – messages intended for destroyers. If it was for destroyers, I think their concept was the battleships should also be able to read them, but not necessarily vice versa. And so I remember this – Mitford Matthews had that problem. Essentially, what it was a generator, a key generator plus-minus, which, in effect, had a clock in it, a synchronous clock, clock work so that the ships could set their generator at the appropriate time. Also he had a principle in there which I have seen. For example, I have an alarm clock, it's an alarm clock and a radio. But it's an alarm clock which if I want to reset it, I got two buttons, a fast button and a slow button. If I push the fast button, the mechanism in there, the electronic just goes around in a hell of a rate until I get close to the time I want. Then I got in on the slow button until I get

exactly the time and then the clock is set. Well, this was built into this key generator, so that if a submarine came up and it was an hour after the key for the day had started and they had to catch up, they could get their generator to speed up very rapidly. And then when they get close to the local time, the current time, slow it down and then use the other. And then there was an indication of a signal which would tell them that they had locked in at the correct time and then they could read their messages thereafter. Now, of course, it's a reasonable idea, but I'm still wondering whether or not that idea in setting these electronic clocks, the fast key that'll speed it up and then catch it, was not a result of somebody in one of the services who was involved in this kind of equipment realized it and got out and got a job in the company. So the R&D requirements was a combination of what our own R&D people came up with as interesting mathematical problems or realizing we needed key generators, secure key generators, different ways of developing key generators also kind of mechanisms which would be secure in rotor devices and things. Plus the requirements which came in from the services that they needed a communication system to meet this and this kind of a demand. What kind of device, you know. Also CSEC would come in with requirements from their security studies. Their handling of the distribution problems of the machine. For a while they used to punch up a lot of one-time tape on one-tape that a whole production. Well, these, these were problems which got to be difficult so they would come to R&D section and say, "Well, there is a problem, what can you do about it?" Eventually, if there was an idea there'd be an exchange and it if meant ultimately a contract for production of devices, the CSEC had its own engineer group also and once it reached a point, let's say, where it was agreed that this was a device which would go into production and then the contracts were let to produce the devices. Then the CSEC engineering group was

responsible for letting the contracts and monitoring it, not the R&D people. The R&D people were essentially responsible only for those contacts which involved research or development, but not production of CSEC equipment.

FARLEY: You anticipated – I was going to ask what the original concept was that the R&D people would devise or develop machines or come up with ideas for machines and then contract it out?

KULLBACK: Well, if it was for CSEC for the use of cryptographic machines, like the AFSAM-9 when it went into production, then whatever new machines have since been developed, at least while I was there, it seems like an excellent idea, the concept was the R&D people would be involved in any contracts which involved research and development. And then once it was agreed that this was the device that this was ready to go into production, then the money for the production contracts and the supervision of the production contracts was handled by the CSEC engineers. A number of the engineers from R&D transferred, like Tom Rowland, who used to be in R&D. When he retired he was in CSEC. Barlow went from R&D to CSEC. I think he became head of CSEC for a while there. Don Frost was in the engineering group production. Let's see, who are some of the others? But these are engineers who had originally been in the R&D side. Some of them had worked really on the R&D of some of these devices and then were transferred or went over to CSEC. Then the supervision of these production contracts were done essentially by CSEC engineering people. They had an engineering staff. And two logics then, a similar relationship existed between R&D and PROD. While it was essentially research and development, developing techniques or contracts with these company to develop means of memory, rapid access memory or high-speed printing devices or the replacement of tubes. The original memory was on tubes. First replacement was by these long mercury delay lines. the information would be passing on a mercury tube at a precise

speed, and you could then look in it and see if memory would circulate. and then got into transistors. We had contracts just first in the development learning all about the transistors. I imagine I would guess the Agency probably got involved in some of these research involving the little chips now, compacting so that you could get a lot of memory and a lot of speed. But this is where the R&D was. Now once it was agreed with PROD that this was the device which would meet their needs, either a special purpose machine or a relatively general purpose computer. Then the supervision of such a contract also involved the PROD people. Either people from the section for which a special purpose machine was being built or the PROD machine group, because ultimately these machines would go down into the machine section and be used, operated by the PROD machine section. This was, I'm talking as of 20 years ago. Some of these ideas seem so reasonable that you would think that they were the main, kept up in some such fashion. If there was an R&D that that would be a distinction. R&D would do research and development and then people who were going to use the output would get involved once they reached the point where you were, in effect, building devices to meet their requirements. They should get involved in the early development of the early stages of those things.

FARLEY: Were there any fiascos, that is devices originally thought to be "the salvation of the world" that ended up as "white elephants"? I stil recall people calling HARVEST originally a white elephant and they used to walk tour groups down and point at it and say it's big and beautiful, but it doesn't work. That was overcome later on, but can you recall any other incidents like that that you'd like to talk about?

KULLBACK: No, I don't recall. I mean even I don't think HARVEST was a white elephant. Maybe it was so big and new originally that there were problems in getting it to

operate, but I think once they got it to operate it did what it was supposed to do, at least what they'd hoped it would do.

FARLEY: I think later on it was told that there was a reluctance of the analysts to use the machine, too, because they didn't know how to go about it.

KULLBACK: Yeah, yeah. No, I don't really recall any device that was built and that really turned out to be useless. Even ABNER was a wonderful learning device, a wonderful learning device for our engineers in how to design and the computing ideas. And it did useful work, once. I think on some of these machines the big problem then was getting the cryptanalysts to learn how to use them. So it wasn't that the equipment itself was really a failure, but the failure was on the part of the cryptanalysts, not learning how to exploit it for their needs. And I don't really recall any device or any large mechanism that a lot of money was spent on and then you say it was a flop because it didn't do what it was supposed to. I don't know, it may have been since then, but not up to the time that I retired.

FARLEY: Can you recall who were the prime movers in the R&D, the outstanding engineers that you recall in the early days – the HARVEST, the ABNER and the successive systems?

KULLBACK: Well, Milford Matthews was one. What a shame when he died. Leo Rosen was pretty fine. Then the group that worked on ABNER. [REDACTED] was a branch chief with Tom Rowland and oh, what's his name, I'm missing one, tall – he's president of, I'm losing my mind. The society of retired people (Mr. Farley tells him the name he's trying to think of) Ray Bowman: [REDACTED] Barlow particularly on the cryptographic side. Let's see if I remember. (Mr. Farley offers Sammy Snyder's name) Well, he was on the PROD, the development side, yeah. He was concerned with ABNER and its being put to use as a cryptanalyst, whereas these other people were concerned with how does one build a device to

(b)(3)-P:L-86-36

do these things. Well, as I say, the superscritcher was essentially a device which used a lot of storage to these very little electron tubes. And the ENIAC which was built by the Census Bureau used electron tubes for storage but it required a lot of power, and heat and air conditioning. So when we started building a computer as a computer, the basic memory in there was the mercury delay lines. That was the advanced, the far-reaching state-of-the-art at that time and from there on it went to transistors and then on to chips and so on. Then I think the Agency stopped. Now ATLAS was the one that had been started by the Navy, the CDC. I think the memory part in ATLAS was still electron tubes because it needed air conditioning to keep the thing cool. But for its day, it, too, was an advanced machine, not only in that it was using whatever the state-of-the-art engineering techniques were available, but also the things, the programs that had built into it for it to do, which were really aimed at being able to use it as a general purpose high-speed cryptanalytic device, see, not just a computer to do ordinary computation. Of course, nowadays, even these little home computers that you get are designed so that they do more than just computation. They can do management data, inventory, a lot of other things that people have built in. But the machines the Agency wanted, of course, were machines which would have the general capability of a computer and yet be able to do all of the cryptanalytic needs, certain peculiar types of programs which nobody would have thought of building into a commercial computer, but which would have been necessary for the Agency. I think Sam Snyder's write ups pretty well tell us some of these aspects, relationship of the Agency machine program development concept to the commercial computers.

FARLEY: What was George Hurley's involvement in the machines?

KULLBACK: Hurley. Hurley was in PROD and so the involvement of the consumer really of the need of the cryptanalyst who would want the machines to do for him certain

kinds of jobs. There are a number of people in PROD who have the ultimate user of the output or an indication of what they would want the machines to provide them in the way of output, were also interested in the development of the equipment because if it couldn't do some of the tricks that they needed in their cryptanalytic operation, then they would need special cryptanalytic devices. I think the Agency's tendency seemed to be towards moving away from special purpose cryptanalytic devices and develop a general purpose computer which could be used on a wide variety of problems. Now, of course, where you need a specific machine like a bombe, for example, if it was a known cryptographic device which is being used, that was something that'd be something else and I would imagine we want to build special purpose equipment. I think for the Hagelin problems, they had special purpose equipment because it was a specific device, but I think as the computers became more sophisticated and can do a lot of things because actually probably program one of these high-speed general purpose computers so that it could simulate the action of the Hagelin and use them for the Hagelin problem.

FARLEY: Do you think as a computerman now that we're relying too much on computers and not enough on the human element in the cryptanalytical area?

KULLBACK: The computer never will replace the human element. All a computer is is essentially as I would describe it, I always have, as a very stupid but very fast and accurate clerk who will do what you program it to do. And all these stories about computer error or that the computer fouled up ain't so. All the computer did was what it was told to do and if whoever told it to do fouled up the instruction, then the computer also did. So all these stories you hear from the telephone company, or from particularly from the department stores that this was a computer error, it's not a computer error. Some clerk who had to punch in the data made a mistake and they got fouled up. No, the computer will never

replace the human in terms of judgment and the important thing that the cryptanalyst has with the computer wouldn't have in working on any cryptanalytic problem when you run into a dead end, what do you do next? The computer will never know what to do next. That's what makes a good cryptanalyst, the idea of what you do next. The computer is a very useful tool. It can do a lot of operations and give the analyst a lot of data to examine and so on. But it still needs a cryptanalyst and his mind to know what the output represents. Whether it is doing right or always the most important thing is, "What's the next step? What do I do next?" The difference between a good cryptanalyst and a run-of-the-mill cryptanalyst is a better ability to decide what is the next likely step as we go along in this problem. That's where Frank Lewis was very good. He was able to say, "What do we do now? What's the next step? So far we've tried this and it didn't work, what do we do now?" The computer would never be able to do that, so I don't think any analyst in any field whether it's cryptanalysis, or in management, or statistics, or anything else has to fear that the computer is going to work him out of a job. That's ridiculous. The computer may make it possible for him to do an awful lot more with his data than he could do if he was either parcelling it out to a clerical trying to do it with 3x5 cards or something else. As a matter of fact, in the past we always found that the computer generated sometimes a need for more people, because you could get so much more data, so much more information that you needed, more people to process and do what the computer was furnishing, because the computer, in effect, was such a large number of people with such a capability of just turning out what you told it to do that it could swamp you unless you had enough people then to process what was coming out. And, I think Howie Campaigne made a number of interesting studies, if they're still in the file. But the progression in terms of the cost per operation as we got more and more

sophisticated computers, the cost per individual operation decreased to such point that we could do for the same amount of money, really, do many, many more operations, get further into a problem, get more data, try many more things. Where it was essentially a kind of a problem in which there was no clue as to which was a more likely so you had to start here and try each of these pads until you found the right one will not work.

FARLEY: If we had computers at the state-of-the-art of 1960 in World War II, how much would we have shortened the length of the war?

KULLBACK: Well, I don't know whether you can say it would've shortened the length of the war, because unfortunately, let's say, even though we might have had state-of-the-art computers of 1960 in 1940, the fighting there still required infantrymen with his rifle. It wouldn't have affected their problems, capturing islands from the Japanese, invading, all of that business. But conceivably we wouldn't have needed possibly, maybe we would even need more. It could have affected the number of people in Arlington Hall Station who processed these things, who did the paper work. If the paper work could have been done, if more of it could have been done by a machine, which is possible because the machines are not a bit more sophisticated, so that people wouldn't have to do so much hand work in addition to what the electromechanical equipment was doing. It might have contributed to faster solutions and possibly with fewer people, but that wouldn't have really affected the outcome of the fighting. The guys still had to get and land on the beaches and fight the Japanese and wear them down and kill off a number of them so he could capture the island and set up the air fields. And that wouldn't have changed by the rate at which information was being processed in Washington, which even for those days was fast enough so that information out to the commanders, or to MacArthur, for future evasion plan, came to them in time enough for them to be able to take it into account in their

planning. Now what to do instead of important information reaching them two days late because, you know we just couldn't get the information out in time. But it wouldn't have affected, I think, the course of the war because if our capabilities, cryptanalytically, hadn't kept up with the needs of the day, then you could say, sure if you'd had machines that sure we could have kept up it could have affected the course of the war. But I think so far as the output from the cryptanalytic activities, the information which was furnished to MacArthur and the Pentagon, and what they knew about the Japanese Army and the strength and capabilities and supplies and everything else, it got to them in plenty of time so that it affected the course of the war in a sense that the commanders, MacArthur had a lot of information about his enemy, he wasn't going blind into a lot of these areas that he invaded. I think maybe that's one reason when they finally got the atomic bomb, they decided to drop it on Hiroshima and Nagasaki. As of those days anticipating the -- I mean the people now, you beat their hearts, their breasts and about the bombing of Nagasaki, how many were killed and the chances are that if Hiroshima hadn't been bombed and Nagasaki hadn't been bombed, many more people, both Americans and Japanese would have been killed. They were then planning at the time an invasion of the Japanese home island. It would have been a hell of a slaughter to be successful, and even though by that time Japan's Air Force and a lot of other capabilities had been cut down and diminished. The invasion of the home land would have been fanatical enough to the point where it would have been very, very bloody. So from that point of view, Hiroshima and Nagasaki really saved lives. Of course, unfortunately it lead the development of nuclear power in the situation that exists nowadays, but I don't know whether you can blame it on Hiroshima and Nagasaki, because sooner or later I think the knowledge and the capabilities of building these things were incipiently in the hands of many countries. And if we

hadn't done it and used it, somebody else would have. The world today, I think relative to nuclear power would have been the same situation, so you can't blame it on Hiroshima and Nagasaki and point the finger at the United States. I think the United States did what had to be done. I think President Truman realized it and I think the decision he made to authorize the bombing, the use of those things was a proper decision. And you see the first, the first bomb didn't faze them, it took a second bomb when they finally realized and got the message.

FARLEY: Sir, in the early days of R&D when you took over, what were the major problems facing you?

KULLBACK: Well, the major problems was first the development of basic computer techniques so that we could build general purpose equipment for the Agency. And so a search in those directions was simply aimed at getting fast high-speed components. Was always trying to reach a level of speed, at least by a factor of two more than the existing ones. And we had a lot of contracts out. the Agency invested a lot of money in research contracts to support all kinds of research which seemed likely a success in different kinds of high-speed memories that you could compact because, again, the limitation of running the wire from here to there simply slowed down the whole equipment. So that was one problem. The second problem was essentially the development of a new line of security equipment, and the first one that was worked on was an on-line teletype, teletype. And also speech and pictures, speech and pictures. Both studies into the properties of speech so that the more you knew about speech the more you'd be able to encipher it in some fashion and then the same with pictures, facsimile. And this was partly in conjunction also with the general purpose computer, but also which would have been used and necessary with any high-speed communication, high-speed printers. Because if your printer was

mechanical and operated at a slow rate of speed, then that was the limit on the output no matter how fast the internal mechanism worked. So you had to be able to try to keep up with the high-speed of the machine itself by printing (?now and so?) That was one of the things we did a lot or work on internally and by contract. Andersen and Nichols I remember was the company that worked and Barlow and Rosen, I think, came up with some ideas which they patented. Eventually those patents were bought by Andersen and Nichols and were the basis of high-speed printers which Andersen and Nichols manufactured for us and for other commercial use. Then the other problems. Let's see, that was the computer section, then we had the speech and facsimile section, and then the section which was trying to build a new line of security equipment. Mostly we were aiming for on-line equipment and, in fact, eventually generated the notion that we had a circuit and there was something going on the circuit twenty-four hours a day. If you had a message to send you just cut in and sent your message. But an enemy intercepting that link...

TAPE VII, SIDE B

...would simply see a continuous stream of off/on signals which when you examine them all looked random and you can't tell when or where a message was inserted along in there. That was the aim, the goal. It meant that in the mathematical research side, a lot of investigation into particularly methods of key generation, mathematical methods of key generation to be sure that the output would actually be random and not think it was random because the way you built it up, actually mathematical properties. Some ideas with respect to rotor machines and in general working on problems which were supplied by

PROD people or cooperating with the PROD people. Of course, the BOURBON, the Russian problem was always in the forefront in everybody's mind.

FARLEY: Was there a shortage of engineering talent in the early days?

KULLBACK: Well, I think we had, let's say, vacancies that we were always on the lookout for good engineering talent. Yes. But there were fortunately a fairly large group that stayed on after the war, so that when we had the R&D section started right after the war, we had enough engineering talent for these various projects that we got started on. But we gradually had vacancies. We were recruiting. Some of the problems from the engineering point of view that we ran into was one. I think that the commercial industry had a need for engineering people also and the grass seemed to be greener outside the government so they could attract engineers. We lost some engineers because they felt that they could do better outside. Also, unfortunately, they gradually developed this notion that it was wrong to work for the military. After all, the military was engaged in planning to kill people and all of that business. So there were some schools, some areas who discouraged, let's say, their graduates from getting involved with ASA because it was a military establishment. Some mathematical groups were opposed to mathematicians working for the military because they felt that you were providing them with a mathematical capability which would enable them to kill more people, kill people. So for a while, and also actually there were some companies that we tried to get contracts with them who weren't very enthusiastic about getting involved with Department of Defense contracts. Now I don't know whether they'd had experience with contracts and the contracting officers and all the rigamarole that went into security, you know, we were also, of course, requiring Top Secret clearances for everybody and so that was another hindrance. But I think we managed to keep our staff of engineers and grew as needed. We were allowed vacancies, we could hire people and then there was

an interchange within the Agency itself. A lot of our R&D engineers eventually ended up in CSEC when developments had reached the stage where we're now ready for production and they needed engineers to supervise those contracts. So really, some of the engineers who'd worked on a thing on an R&D project transferred to COMSEC. And I think the same thing was true. Jimmy Fuld ended up in PROD. Some of the people in other problems and the radio intercept section. Who was the head of it? He is now President of AMPEX. Hoffman. I think it's something like that. Hauseman. Hauseman? He was head of the radio intercept. You mentioned about problems. The problems that we were working on then in the radio intercept was one, how to intercept microwave signals from as far away as possible -- the line of sight signals. That was a problem because we couldn't necessarily [REDACTED]

[REDACTED] So we did a lot of work there, and also with wideband tape records, which ultimately developed into the kind of taping systems they use now on TV. In fact, two of the engineers, Robert Sackman and [REDACTED] eventually left NSA and went to AMPEX and were very responsible for AMPEX growth and development because they got a toehold on the wideband, wideband receiver, yea. The idea there was again a requirement from [REDACTED] section in PROD, the intercept people, of trying to get an intercept receiver which would have very wideband capabilities and then copying everything, which was on the air and then later going back and studying it to pick out or maybe you weren't interested in that traffic today, but maybe six months from now, a problem would arise in which you would want to have that traffic. So at least you could have a way of storing it. I remember we would take some of the equipment and intercept what then was [REDACTED]

(b)(1)  
(b)(3)-50 USC 403  
(b)(3)-P.L. 86-36

(b)(1)  
(b)(3)-50 USC 403  
(b)(3)-18 USC 798  
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)  
(b)(3)-50 USC 403  
(b)(3)-18 USC 798  
(b)(3)-P.L. 86-36

[redacted] Also actually, doing tricks by shooting up rockets and shooting out ionized clouds which would leave very pinkish colors and the [redacted]

[redacted]

And, in fact, many of the experiments which were carried out at Wallops Island, I think, in which the night sky sometimes would be lit up with these very colorful clouds, were a part of it. They were carrying on a program of their own for research on atmospheric conditions and so on. But also when these ideas were routed about so [redacted]

[redacted]

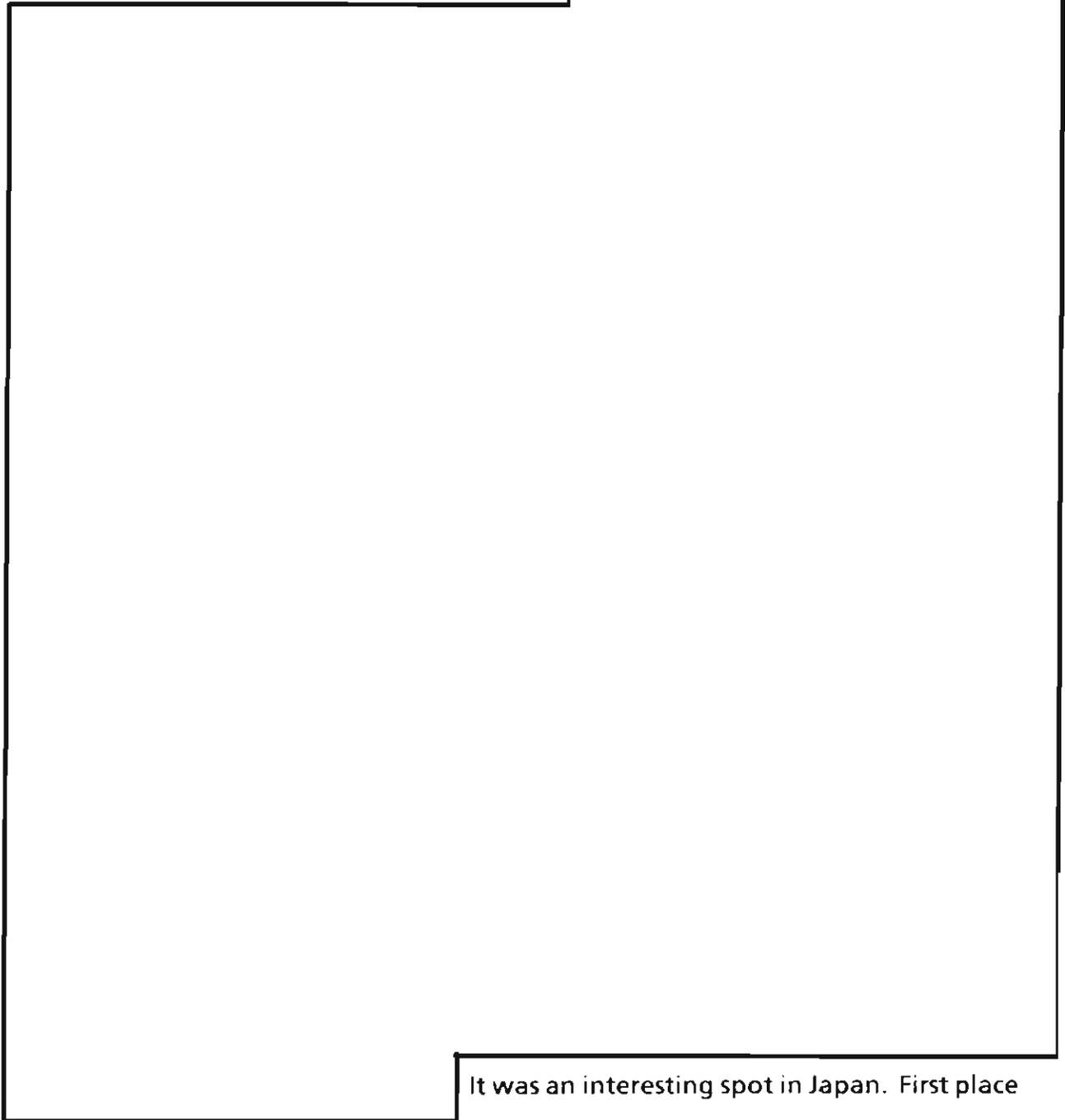
I don't know that a lot ever came of them because, ultimately, other means were developed [redacted]

[redacted]

FARLEY: Did you do much work with satellites?

KULLBACK: No, this was really before the age of satellites. I imagine later on when the satellites got in, the Agency got heavily involved with a variety of new problems which came about when the satellites came in. But I left in 1962 and as of that time I think maybe the Russians had sent up their first sputnik ((1957))and the United States was engaged in the high-speed program to develop satellites, but never got involved while I was there. I would guess from things that the Agency now is probably heavily involved in with satellites, with security of satellites, satellite communications. Oh, there was another project that the intercept

people were involved in jointly with PROD.



It was an interesting spot in Japan. First place it got an awful lot of snow so in the wintertime you were up to your ears in snow. We went there, of course, in the spring. It was really rural Japan – away, way away from the normal tourist, no tourist could get that far. In fact, to get up there if I remember you took a train in Tokyo to Sapporo and then changed to another rattle trap. Japanese trains weren't too bad with sleepers. They

provided you with a kimono, slippers. You could travel without a suitcase and have all that you needed. Then eventually picked up by military vehicles and taken out to that station. The interesting thing which, I guess, was true in the Far East which was noticeable then, there were a lot of road work going on. They were fixing up the roads and all of the heavy labor was being done by women with little baskets and carrying the stones. The men were sitting off on the side, whatever machines they had eventually when they had enough of this, and had to grade it down. The men sat comfortably and hoards of women doing all of this heavy labor. And, of course, this was till sort of post-War Japan, when Japan was under the domination of the U.S. It was a different kind of situation and for Americans in the military service were really treated quite well. Of course, they kept an eye on you. I landed in Japan, my wife had gone through. That's when Sally was working at Zama and she had gone out to take advantage of the fact I would be there also. She had flown and was staying with Sally at Zama and sure enough when I came through Tokyo – Oh, yes, you wife had gone through, they knew this damn business. And that was interesting. You visited a military establishment, first thing Japanese women would be there to take your dirty laundry and within the next day, they'd bring it back all neatly ironed and pressed and everything.

FARLEY: I am amazed how they can keep each individual straight so they knew whose laundry was whose.

KULLBACK: But they managed that.

FARLEY: Did you ever work with any lasers at all or did that come later?

KULLBACK: No, that came later. Not in our time. Well, it was not available. There had been a lot of developments. Remember it's twenty years since I retired.

FARLEY: Trying to sort it out in my mind.

KULLBACK: No lasers. Hadn't reached a point yet where we'd be thinking of working on that. And then we were trying to push the state-of-the-art of getting people interested through research contracts to push the state, particularly into the computers, and high-speed memories, random access memories, high-speed printers, circuitry. These were the things that were of great interest to us so we could have much greater capability, general cryptanalytic equipment, plus the security studies.

FARLEY: Where will it end?

KULLBACK: I don't know. Just keeps on going. Doesn't look like it'll ever end really.

FARLEY: Let's see, what would you say was the most satisfying accomplishment in R&D when you were the Chief of R&D? What are you most proud of?

KULLBACK: R&D? Well, one was the, to a certain extent, the AFSAM-9. I mean I really did yeoman's work for on-line communications. I think we contributed a good deal to knowledge about speech, speech make-up. Some of our mathematical people did a lot of interesting mathematical work in the key generation process. Mathematics of those things. We did build a lot of special intercept equipment for PROD: [REDACTED] was our biggest consumer on those things, and so did actually contribute to what is a very big commercial thing today which is really the tape recording for television. I still remember now, talking to Leo Rosen one day about using magnetic tape. [REDACTED]

(b)(3)-P.L. 86-36

So I

dropped it. But, funny also, I remember when Sackman left NSA, it was ASA (?AFSA?) still at the time he went. He got this offer of a job with AMPEX, and he was concerned. We had lunch and he asked me about whether or not he was making the right move in getting in there into tapes. And so this was in the early

days of magnetic tape. I think we had gotten knowledge about recording what the German recorded, we've gotten and seen were just on wires, strips of wires and then getting on into these little narrow strips of tape for recording, speech and other things. And I said that I had felt this was a direction which would really expand and for an engineer to get into it early like this, had tremendous possibilities in the future, which is exactly what happened insofar as AMPEX and his own job in AMPEX was concerned. He came out with an awful lot of money from his AMPEX connections and knowhow in tape. Of course, AMPEX made a hell of a lot of money as they got into these developments, particularly when they finally got a practical tape for TV, so that now they get all the tricks they do, all their playback and everything else under this sun which can be done.

(b)(1)  
(b)(3)-50 USC 403  
(b)(3)-P.L. 86-36

[REDACTED]

I think the Agency had a hand in that development, computers, plus an awful lot of the mathematical work. I mean after all, I think the contributions which IDA made up – the Princeton. They made a lot of contributions as part of the whole R&D. So I think there are a lot of things we accomplished that one could be proud of. No need to hang one's head in shame.

FARLEY: Were you chief for what, ten years?

KULLBACK: R&D?

FARLEY: 1952 to 1962?

KULLBACK: Let's see. I retired in 1962, right? I was Chief of R&D – when did we move into Ft. Meade?

FARLEY: 1957.

KULLBACK: 1957. It was before that. I became chief, because there I was involved in the move of R&D out to Ft. Meade, so it was at least five or six years as head of R&D.

FARLEY: So what did you do between 1952 and 1957? You were a Technical Director within R&D?

KULLBACK: I was within R&D. The reorganization after the war, I was in the R&D activities all the time, but as a Technical Director. The head of it was one time a Navy, where we first had AFSA, the Army and the Navy got together. I guess they couldn't conceive of a civilian being over a Navy captain so he was the Director, and I was Technical Director. Then when he retired, when they brought in Clarke from Bell Labs, from outside, I was continued in the position of a Technical Director and then when he died, instead of going outside the Agency for a director of R&D I was appointed. When I retired, Matthews. When he died, unfortunately, one of the branch chiefs, I think, became chief.

FARLEY: I don't even remember who replaced Matthews. I don't even know who the chief of R&D is now.

KULLBACK: I think the chief of R&D since then has essentially come from within the Agency. Initially General Canine thought of going outside and bringing in from Bell Labs, but I don't know whether he thought the getting a retired person who then died, or whether we could do it internally, was a better idea. I think thereafter the Agency brought up its own people.

FARLEY: Did we get any useful talent from outside the Agency? That is from Commerce, I don't mean from Commerce, from commercial enterprises or organizations that we used to contract to - people who thought it would be better to work for the government? We have in place a lot of contractors now. I don't know if this was developed during your tenure.

KULLBACK: You mean they are contractual people but they're working in the Agency?

FARLEY: Yes, and some of those people resigned from their corporation and took employment at NSA, which is surprising, it's sort a reverse trend.

KULLBACK: What happened was that with some of our contractors, particularly in the computer field with IBM, some of the IBM people were stationed and had desks you might say in NSA for liaison with the activities going on in their company. But they weren't really in NSA, working for NSA by contract. I think this thing you mentioned is something that developed afterwards.

FARLEY: Probably.

KULLBACK: Later on. People come to us. Well, we did get some in our recruiting efforts for engineering talent particularly. We did get some from outside, you know, visiting places where we had contracts, but in the main, I think, if there was a flow it was Agency engineers going outside. They thought they could do better outside and the Agency would hire engineering people and then develop them in their own skills within the Agency.

FARLEY: Was there any program ever developed where you could control an engineer after spending four or five thousand dollars to send him to school to get a masters degree, then he comes back and works for six months and then goes to industry?

KULLBACK: The only general understanding for mathematicians and other people that if the Agency sent you to school for a year, when you were finished you came back and put in at least a year with the Agency.

FARLEY: Oh, I see.

KULLBACK: I think that's what it was year for year.

FARLEY: So they were required to reimburse in time.

KULLBACK: Well, that's, yes. I mean the understanding was if the Agency -- the Agency I think starting with General Canine was always in the forefront of educational opportunities for its employees, like they had these scholarships and other things. And there were any number of people that got Ph Ds or other advanced degrees as part of their Agency assignment. And I know Bill Blankenship, he's

since retired, went to Princeton, got a Ph D in mathematics and came back. Some of the people that we went away for these educational programs came back and griped like hell for the couple of years. I know one in particular, a statistician. He was sent to Stanford University. He had been studying here at GW and spent at least either one year or two years at Stanford. The final years the Agency supported him, he got his Ph D and then, of course, had to come back and work in the Agency for the equivalent length of time that he had been supported at school. And he was griping all the time. No consideration of the fact that, after all he had been supported and a lot of money invested in him for him to reach the high level of expertise which he felt he had, and continually griping that he could make more money outside. Eventually the first opportunity he had, he did leave. I mean, he's done all right for himself in the academic world, but the same token it seems to me he had exhibited a rather ungrateful attitude. Okay, if you feel that now you've developed a certain expertise, the Agency did send you, give it back in terms of time anyhow, a year or two that you had been given an opportunity. He was a married man with children, so to be able to go to school full time, get his salary and everything was something which he shouldn't have griped about. Then come back, put in your year or two and in the meantime if you look around and find you get an opportunity to work in the academic world, all right, but don't spend that year or two years grouching all the time because you were working in the agency that had supported you, when now you felt that you had the expertise, you ought to be able to be outside. But we had no other program then other than the general understanding that for every year that the Agency sent you to school, you should give the Agency back one additional year. In other words, don't get your graduate degree and then go off. Come back and give the Agency at least a year of service and then either stay on or go about it. But this is true and I guess this

the general practice in the military -- in the Army. If people during their military career are given special schooling, then the service expects that you'll stay on for at least as long as the training that special training was given to you.

FARLEY: You're committed for that time period.

KULLBACK: But now I don't know. Suppose an individual was sent to a school for a year and then said, "The hell with ya, I'm not coming back to work." What recourse the Agency or the services had enforced, I don't know whether they make them write an agreement, or contract or whether it's implied. Of course, if the individual has money due from the government in retirement, I guess the government can put their fingers on it or something like that. Otherwise, I don't know that they have any way of really forcing the individual to or what powers they have to force the individual to repay in terms of time what the government spent. Now I don't know whether they've solved the problem now or not because I know the Agency has a big educational program of sending people, fellowships and everything.

FARLEY: Got some good schools in almost all areas, too.

KULLBACK: Whether it's a problem to the Agency or whether people are appreciative enough to be given an opportunity, at least to pay back in terms of the time.

FARLEY: What are other areas in the R&D we should cover? What else would you like to put on tape? Any criticism of the programs, or the way it was run under different Directors while you were there? Did you notice any change because a director or deputy director may have been inclined toward R&D, or disinclined? Did you notice any change about?

KULLBACK: Well, the only changes I can think of -- all of the directors and the deputy directors appreciated that we had to have an R&D program. I think the biggest differences were essentially their outlook on publications. General Canine felt that some of the papers which Agency people would write on fairly esoteric

subject. In other words, that didn't deal directly with the cryptanalytic activity, but in some of the physics research. We had a physicist who we'd hired from MIT who was interested in some esoteric side of physics, molecular structure and things of that kind and wanted to write a paper with an indication that he was at the National Security Agency. Now for a long time things like that were verboten. If you wrote anything at all, first of all you had to be sure that it wasn't obviously a cryptanalytic problem, cryptographic problem, and you didn't put down the National Security Agency. I had statistical papers published while I was working at the Agency but I was teaching part-time at GW so I would always sign myself as George Washington University and in an abstract statistical thing which really had no direct bearing or relation with cryptanalysis. General Canine felt that if the Agency had people who were good enough to be advanced in certain areas and be able to write a scientific paper for publication, but you know nothing which would in any way risk security of the activities, he felt that he would just as soon have the paper published as a National Security Agency employee. Because he felt that such things would, you know, redound to the credit, not only to the individual, but to National Security Agency. National Security Agency, let's say, had people who were far more knowledgeable in these esoteric branches of physics could write this paper which would be accepted by a standard physical journal and so on, be published as a scientific paper. Some of the other directors had sort of different outlooks on security.

TAPE VIII, SIDE I

KULLBACK: They mabe didn't object if a paper was published in a scientific field which didn't reflect directly and obviously on the mission of the Agency. For example, if somebody could write a statistical paper or abstract statistical paper which had

nothing to do with cryptanalysis, some of these directors felt that it could be cleared, to be published, but not as an NSA employee. So the individual would list his name, with no association, the Department of Defense maybe, but no association with National Security Agency. That was a big difference, the biggest difference at least that I can see. Now there may obviously be other differences in the point of view of the succeeding directors and also in their relationship with their services, but one of the biggest differences was their outlook on questions of security. General Canine, I think, took a broader point of view, not that he said security's not important, but he tried to think of it in terms of reasonable. For example, he felt the fact that an NSA employee could write a highly esoteric technical paper in the scientific field, he was glad to have National Security Agency listed as a place where this employee worked. Some of the other directors just didn't want National Security Agency appearing in any publication, any kind of publication. And, of course, this is what caused Mr. Friedman a hell of a lot of trouble. He was always being approached. When people thought about cryptography, Pearl Harbor or anything else, he was the man that a lot of the government agencies or in the newspapers thought about. He was the National Security Agency. And very often, I guess, his name would appear in connection with National Security Agency by some guy who was writing an article, Mr. Friedman wasn't even consulted whether he could use his name, and some of the directors were a little upset at simply the publicity that NSA was being in the public realm. Of course, to a certain extent the less often National Security Agency is mentioned in the newspapers, because they always describe it National Security Agency Super-Secret Organization involved with all kinds of intercept activities, this, that, and the other thing. This is not what the National Security Agency want to appear in the newspapers for all the time. But unfortunately with those buildings out at Ft. Meade and everybody can drive

by and see National Security Agency and they jump and draw their own conclusions which are sometimes pretty far-fetched. This question of security is one which concerns the directors to some extent. Some of them react to it with a reasonable point of view, some of them maybe go a little bit overboard in their problems about what they think of security.

FARLEY: What do you think of a man like Wayne Barker of the Agean Press being able to sell your paper for \$15.00, I think it is? The one that you did on cryptanalysis, I believe.

KULLBACK: Well, we should have copyrighted these things.

FARLEY: Yeah, it's a shame.

KULLBACK: But at the same time, I don't think any government publication, through the Government Printing Office, can be copyrighted.

FARLEY: That's a shame, he's collecting money on something that you sweat and toiled over for quite a while.

KULLBACK: He's in business for making money and there's no way we can, if it isn't copyrighted, and it isn't classified, then there's really no way in which he can be prevented from publishing these things.

FARLEY: It's a shame.

KULLBACK: He had an idea. He used to be at the Agency and he apparently was able to manage to get hold of a number of these things, so he exploited it for money. Money is the root of all evil.

FARLEY: Kully, is there any possibility that you can come out to the Agency and help identify some of the old equipments and machines that we have on the racks that have been collected from Mechanicsburg and all over? We want to get your opinion on what they are. I mean when you get straightened out.

KULLBACK: Well, I mean, let me get straightened out with all these damn hospitalizations coming up. I have one coming up on the 21st with this catheterization and then

hopefully after that I'll get an operation and get these polyps removed out of my nose so I can breathe a little better. So that if I could get these things straightened out I'd like to come out there and find out what some of these equipments are, if I could remember them. If they go before '62, recognize what they were, where we got them. Just let me get over this damn – for a while I swear there were periods here when I had as many as three appointments with doctors in one day. Kept them all coming.

FARLEY: Well, I hope it comes to a head satisfactorily soon.

KULLBACK: Quite a mess. I still don't know what might be the outcome of this angiography that they were going to perform. They may recommend they undertake a heart by-pass, the by-pass you know – open heart surgery with a by-pass. I don't relish even thinking about it.

FARLEY: No, let's hope not, let's hope a little more medication will take care of it.

KULLBACK: Medication will take care of these things, but with all these things staring me in the face, and in the nose, I hate to make any firm specific promises as of now.

FARLEY: Well, let's put it on hold. Is there anything that we've overlooked? The only think I could think of is the days at the end of the war and the phase-down of the ASA. Is there anything that we should put on tape about what you went through then or is that...

KULLBACK: Well, the last days of the war I think represent – let me give some things on security.

FARLEY: All right. Good.

KULLBACK: I always felt that the real dangers to a security agency, the leaks, would generally not come from people in the agency but from some of the political figures outside the Agency who had access to some of the product of the Agency. And I think this is pretty well indicated by some of the things that did take place. Because when an individual in a high political position makes a statement the

press will hop on it. If some low Agency employee were to say the same thing, we would pooh pooh. What does he know what he's talking about, and things of that sort. Within ASA ((SSA)), twenty-four hours before the official announcement of the end of the war, Japanese were going to sign it, because we've been reading all of the Japanese traffic and finally their offer to surrender, the answers and all of that business, and when the time had been set and so on. Now again, I think even at that late stage, General Corderman's reaction was to lock the gates, not let anybody in or out, and disconnect all the public telephones and not let any outgoing calls or incoming. In other words, isolate the Agency, not to have any communication and I think he was talked out of that. And no word leaked out of anybody in ASA ((SSA)) where practically everybody, everybody in the Agency knew, in other words that things was in a Japanese section, but the word got around. Nobody, nobody outside the people in the Agency had any inkling about what happened until Truman got on the radio and made the announcement. So again, I think this is an indication of the responsibility, at least at that time, the responsibility of the people in ASA, ((SSA)) their responsibility to the Agency for the security of information which they got which shouldn't be leaked out. Now, of course, now the Agency is so big. There's so many people who keep on griping, most of the notes in that monthly newsletter have to do with people who are griping about this that and the other thing. So I don't know whether the same would be true today. But thinking back in terms of the group of people who had been fighting the war through ASA ((SSA)) and the responsibility of their actions. At first the General Corderman didn't trust them to that extent and yet he was talked out of it. I mean it would have been a hell of a lot to try to lock everything up inside that Agency. Not a word leaked out and when the announcements were made, the newspaper published it, that's when it was generally known, even though we

knew about that. I don't know approximately 24 at least 12 hours, something like that, because we were reading all the messages, the exchange of messages which was involved. I would say everybody in the Agency at the time, the news, you know, that rumor mill gets around so fast it isn't even funny. But nobody thought of going to tell, calling home or telling his wife or anything else.

FARLEY: We were extremely security conscious.

KULLBACK: I think they were and in general even though it hasn't worked that way, I think there were more risks to security, not from the general mass of people in the Agency, but from the high-level political. Unfortunately the whole security structure just turned around really. So much security is heaped on the poor guys in the Agency and the higher-level politicians really aren't affected, except Dewey, of course, after being told about it. This was quite a concession on his part because conceivably had he broadcast what he knew, that sort of thing might have made a change in the election, might have made a change in the election.

FARLEY: Might have been a longer war, too.

KULLBACK: Oh, yeah, hell of a lot of difference.

FARLEY: We don't need the Jack Andersons, either. that type person.

KULLBACK: Unfortunately he can't operate unless he gets people in who are willing to talk to him.

FARLEY: What about the defectors, Martin and Mitchell?

KULLBACK: Oh, Martin and Mitchell – that was a bad case. Well, they came, they were cleared, they went through the usual clearance procedures. I guess, but I don't know, the clearance procedures are so air-tight that nobody of that ilk could – – actually we haven't had too many.

FARLEY: Did they work in one of your sections?

KULLBACK: Yeah.

FARLEY: Both of them?

KULLBACK: Both. In fact, one of them had a letter of commendation signed by me. He did what I commended him for was tactic mathematical work for which he had done well in, no question about it. But now unfortunately there, too, who suffered by that? Well, they jumped on our personnel director, Mo Klein, and the head of security. What was his name? He's still with the Agency. He's still alive. They found some piddling excuses to fire them and, of course, the real reason they fired them was because -- why they could have fired me, too. After all, these people worked for me, but after all, once we in the Agency had no control over security whatsoever. We took what people and we were told, this man is secure for this and that, so we took their word, so we had really no way of checking their security. Security clearance was the responsibility of security people. But I think Congress, the committee in its anger and frustration, here are two people who got way, got to Mexico and then got to Russia. They took it out on our personnel director and the security director. And they found some slight askew. If you look into anybody very carefully with a microscope, you're going to find a little something and they just used that. I guess they couldn't use as an excuse that the Agency cleared two defectors. But I don't know, I think one of them has had second thoughts and was trying to get back into this country.

FARLEY: I think he was examining what sort of punishment he'd have to face if he came home. I don't know what they ever did about it.

KULLBACK: I think they really ought to punish him. I really don't know that he could give them an awful lot of detailed information about what was in the Agency. Certainly not about our own security systems. I don't think they knew enough to be able to compromise our security systems, or about everything which was going on. I guess the biggest thing in the newspapers was the newspapers jumping to all kinds of wild imaginings from a word here and a word there

about what was really going on at the Agency. No, then, of course, the other defector we had, well, he really wasn't a defector. What was his name now –

FARLEY: The guy who killed himself?

KULLBACK: No, he spent seven years in jail or something like that.

FARLEY: Peterson?

KULLBACK: Peterson, yeah, Peterson, yeah. He wasn't trying to tell anything to the enemy, but he thought he was friendly with a Dutchman and apparently

(b)(1)  
(b)(3)-50 USC 403  
(b)(3)-18 USC 798  
(b)(3)-P.L. 86-36

which was strictly illegal and all of that business. He spent, what's it, seven years in jail, I think. He's out now, I think. No, I think actually considering 1930 to the present day, there really been, I guess even one defector so to speak is too many, but considering all of the people that have gone through the mill I think the responsibility of the people who've come into the Agency is a credit to the population for and a credit to the Agency and its activities.

FARLEY: Did you know what's sad out there is there's no leading talent like yourself and like Sinkov and Rowlett. Some of the people who were there at the beginning. There's no one individual who stands out, who can be looked up to as, as I said, the leader. It's a shame, but it's the young generation, I guess.

KULLBACK: I'm surprised. I would have thought we had so many good people coming in, and certainly sort of rise to the surface.

FARLEY: They're not of the caliber. Maybe it's because I know most of these people and I'm prejudiced.

KULLBACK: Well, might be. No man is a hero in his own town, so to speak.

FARLEY: Well, Kully, I hate to cut it off, it's been enjoyable. But what are we talking about again – TOP SECRET stuff? Most of it is SECRET. What do you think?

- KULLBACK: Well, a lot of these things have never been published. I don't think should be published and talk about things which were at one time were ULTRA classified. I guess they should be considered as sort of TOP SECRET.
- FARLEY: I'll still make these tapes TOP SECRET COMINT CHANNELS, right?
- KULLBACK: I guess they should be. Now some, if you go through it, maybe some comments which don't deal directly with activities could be extracted and interesting non-classified items. But in the context of all of these things where we're talking about things that went on and have never been published and probably never will be published, I guess it's sound to be on the safe side, is to consider them as still TOP SECRET.
- FARLEY: Should we plan on another session later on where you could talk about the volume of books, the exposes, the various "fibs and lies" that these people are telling? Would it serve any purpose to go into any more detail? Whatever you think. Or would you prefer to think about it and maybe you have some ideas.
- KULLBACK: Well, why don't we leave it. I have some things I would like to say about these people.
- FARLEY: Yes, all right.
- KULLBACK: Write about a business that they'd never been in, don't know, and well, like what's his name? The guy who wrote *THE CODEBREAKERS*.
- FARLEY: David Kahn.
- KULLBACK: David Kahn. I had lunch with him one time. My son was sick in the hospital, and talked about some things and asking a question like, "How does a cryptanalyst spend his day working in the office?" So I told him, like any other scientist working in a laboratory or in the statistical department. But I mean the fact that he had to ask such a question gives you some idea of their distorted view of such things and, of course, some of it appears in their books where they're trying to guess and visualize their impression of what goes on behind the walls that they

don't know what went on behind the walls. See you get some of these peculiar silly statements which appear in the literature.

FARLEY: Maybe by that time you will have read *THE PUZZLE PALACE* by Bamford.

KULLBACK: No, I didn't know about that.

FARLEY: It's on the street.

KULLBACK: On the street – paperback?

FARLEY: No, it's \$15.00 or \$18.00. May be at the library – get it at – it's not worth buying.

KULLBACK: Well, that's the problem with a lot of those books. After I, some of these after I bought I thought not worth buying. Now, for example, *AT DAWN WE SLEPT*. That book can be condensed to half the size and portray what really he wants to say. He's got a lot of the things in there to say, but he spends so much of the first half of the book about the day-by-day arguments that went on in the Japanese Navy about whether to bomb Pearl Harbor or not and all of that business. I don't know that that really contributes much to the whole problem. And most of it is based, or a good deal of it is based, on talking to people ten years after the fact and their picture of what really went on is so unbiased that they become smarter than they were when, so I mean. Well, I guess that's true with anybody who's writing what's presumably a history.

FARLEY: Well, that's good. That'll give you a chance to think.

KULLBACK: Well, all right. As I say, everything depends on what comes out on these forthcoming hospital visits and so on. Spirit has set me willing.

FARLEY: Good, well, that's wonderful, and it's been a pleasure. I'm sorry to keep you so long.

KULLBACK: It's all right, enjoyed talking about these things.