OC-78
TILTMAN, John

format

13 December 1978

Schorreck: Brigadier, if I could, let me put some names to you and if anyone strikes a bell, we'll stop and talk about it a little bit. How about Admiral Hall?

Tiltman: I never had anything to do with Admiral Hall. He'd been right out of the business before I came in.

Schorreck: Before you actually got in in 1920?

Tiltman: Yes, so that what I know is general knowledge. "Blinker" Hall.

Schorreck: Um hum...The rest of these are going to be from the U.S. side, and we'll just see what happens. How about Ralph VanDeman?

Tiltman: Never heard of him.

Schorreck: Marlboro, ugh Churchill?

Tiltman: No.

Schorreck: Parker Hitt?

Tiltman: Parker Hitt...I knew that he...I read a book of his.

Schorreck: The Solution to Military Ciphers?

Tiltman: Yes, something like that.

Schorreck: How did you find that when you read it? Did you find it instructive, or informative, or not much value?

Tiltman: I'm a bad reader in this subject. Nearly all the books I've ever seen have been just awful, but there was a lot of stuff in it, yes.

Schorreck: How about Joseph Mauborgne?

Tiltman: I just met him at Mr. Friedman's...I was staying with Friedman. Met him once.

Schorreck: Carl Kinsley? Captain?

Tiltman: No.

Schorreck: Russell Wilson - a Naval Officer - Commander?

Tiltman: I don't remember.

Schorreck: Milo Draemal - also a Naval officer?

Tiltman: No.

Schorreck: Dennis Nolan, who was Pershing's G-2, who made a trip to London on intelligence matters?

Tiltman: That must have been in World War I. Well, I wasn't in that.

Schorreck: Hooper, J. S. Hooper? Another Naval Officer?

Tiltman: No.

Schorreck: J. Reeves Childs? He was...

Tiltman: He's not the Childs ~~that~~ who's in COMSEC now, is he?

Schorreck: No.

Tiltman: No. Childs, Childs...

Schorreck: John Manley?

Tiltman: No.

Schorreck: How about Safford? (covered in 04-78 1 Nov 78)

Tiltman: Safford, I knew fairly well.

Schorreck: Could you relate to us when you first became acquainted with Safford?

Tiltman: When I came over here in 1942, in March 1942.

Schorreck: Well, let's save that until the World War II period. I think you mentioned before that you didn't know Yardley nor Friedman until World War II?

Tiltman: No, I never met... Friedman was supposed, you know, to come over to England when Sinkov and the others came and he had a nervous breakdown and Sinkov came in his place.

Schorreck: I have one other general question about this early time period -- were you involved at all in wiretapping? British involvement?

Tiltman: No. ~~Never?~~ Not that I know of.

Schorreck: So, prior to the advent of radio intercept, it was all cable drops and then radio intercept came in about 1920, or must have been earlier than that ... before?? War?.

Tiltman: I only came in...

Schorreck: Your association with it came in 1920?

Tiltman: Yes.

Schorreck: I think last time we talked about your efforts from '31 to '34 on the COMINTERN, and you related some specific instances out of that.

Tiltman: I could go into a lot more detail on that, but I have written it up in the journal. I think that one thing that has never been said there is that in 1931, I really took it over from Fetterlein who was not getting on very well with it (the COMINTERN). At that time, we were only looking at Berlin with Moscow and I took it over from him and I originally came in and broke the Berlin/Moscow link.

Schorreck: Yeah, we have that. Could we get into what we were talking informally about a minute ago with how you got into breaking the JN-25 indicators in the late '30s?

Tiltman: It goes back to the beginning of my work on Japanese. I think either at the end of '35 or the beginning of '36, I was getting military intercepts back from Hong Kong which were not being worked on by anybody else and this was before they used additives. They had various systems, more or... greater or less complication which I kept in touch with until September, December 1938 when they began to use the kind of additives that they used all through the war and which I broke into during the Munich crisis, December '37, it must have come into use.

It started coming into use because I broke the indicating system when we were first at Bletchley Park during the Munich crisis. Well, then, this indicating system they used usually, I think, the first 4-digit group of a message they had two figures of it... two figures of the first group of messages, led to one of a hundred additives which was added over the two indicator and put in the second place. They did the same thing for the end of the message and I eventually established that there was a connection between the beginning and the ends of messages which started and ended on the same page. From that point on, the additives were very badly used. We first of all broke into an air cipher which was named "3366". It was very badly used; the first page was very much overused and there were other places, and we were able to read depth. Then sometime just after we were in the war in '39, I should think, as a guess, in October or November '39, we got some Naval intercepts in what was afterwards called JN-25, and I tried to see whether it had a similar indicating system to the military, and I found that it did. It indicated the beginning and the end of messages on the tables...on the key. About that time, Commander Burnett, who was one of the - was really the best of the Japanese Naval interpreters...Naval Japanese interpreters, was sent out to Singapore and he took the indicating system with him and my question to you before was...I didn't know that it had ever been solved...whether in fact they got the indicating system from me or whether they broke it independently? My guess is that they broke it independently. Burnett always swears that they got it from him, but I...

Schorreck: Burnett went to Singapore or to...

Tiltman: Well, he went from Singapore to Corregidor. At that time, he says that he handed over the indicator system; that they didn't have it at the time. I think he's probably wrong. I don't know the answer to that.

Schorreck: Could you recount for us the incident which took place in '37, when you yourself went to Hong Kong to give over some Jap military material?

Tiltman: Yes. It seemed to me...this actually was before they introduced additives. It seemed to me that this was something that ought to be done and dealt with...it was intercepted in Hong Kong and just as the Navy did their own exploitation in Hong Kong, that we ought to have a military party dealing with military in the Far East and not with us. So, I got permission; I went out by sea to Hong Kong and when I'd been there a short time, I found there was really an awful lot of work to be done, working in the dockyard and I found a very good Japanese interpreter, ~~in the...~~ an Army interpreter in a battery on Stonecutter's Island, which is in the middle of the harbor in Hong Kong, where the military intercept was taken. I applied for Marr-Johnson to be attached to me, and the first time I applied, it was refused. The second time was after the Japanese had come down into China and they agreed to let me have him half time. And then when he just got, not only interested but useful, they took him away from me for a translating job in

North China. I was so angry that when I got home - November '37, I think - I made a row in the War Office and they actually flew him from Hong Kong home, so this was an absolutely unknown thing for junior officers in those days, which took a week anyway. I flew out again and I kept him for the Japanese and one of the other attached officers, Geoffrey Stevens, who is an Italian scholar and had been with me for 2-3 years...I put them both onto ~~to~~ Japanese and as soon as they were familiar with what was going on, I flew out to Hong Kong and they followed me by sea and took it over. As far as I was concerned, I dropped shot of the Japanese problem, for the time being anyway. If something was going to be done, I didn't....

Schorreck: Were you ever called upon to....

Tiltman: I beg your pardon...I am getting into a muddle here... They didn't fly out until the beginning...I didn't fly out until the beginning of '39 when we had gotten the indicating system of the additive system, and as this was something that was likely to expand and last forever and was then a fairly well-known procedure, we arranged for Marr-Johnson and Stevens to take it over as a continuing commitment in Hong Kong.

Schorreck: Right.

Tiltman: I got muddled over dates before.

Schorreck: That's all right. Once that occurred, once you had turned the activity over to Johnson and Stevens, were you ever called upon as a technical consultant to them - did they ever ask you for advice?

Tiltman: Not really. What happened was, that, after Pearl Harbor, the Indian Government formed - set themselves to form a cryptanalytic party in New Delhi and the Director of Military Intelligence, General Cawthorne, wrote me a letter asking ~~me~~ who he should put in charge of this, and he named four names and Marr-Johnson was the only possibility; so Marr-Johnson became a Lieutenant Colonel and was the technical head of WEC, which was the name of the party in New Delhi.

Schorreck: Wireless Experimental Center.....

Tiltman: Yes.

Schorreck: So, from that time on, then, for all practical purposes, everything was done out there.

Tiltman: Yes. Where I came back into Japanese, ~~was~~, I was heavily involved in the breaking of the Japanese military attache system, which was quite a different thing altogether. In 1933, I broke into the current Japanese military attache system, which had been going for 6 years. It went out of use just about the time I broke in and wasn't really touched again until about the time of Pearl Harbor. Well then, after the fall of France, we had had...since the beginning of the war, we had 14 naval officers...14 French Naval Officers and 4 French Air Force Officers in Bletchley Park with us and after the fall of France, the head of the Air Force party, Baudouin, who we have a book of his that's been translated on cryptanalysis, Baudouin came to me and said, "We are four very highly trained research cryptanalysts... you're stuck with us for the war. Give us a problem that you

haven't got time to do.". So I gave them the Japanese military attache system and they made such a mess out of it...unbelievable. When I took it away from them again, you could hardly read any of the intercepts. They were all scrawled over with red letters and so on. I had to go back to the beginning again, and then it hadn't been broken when I came out. In March 1942, I knew something about the indicators and Sinkov's party had made some progress with the indicators. One contribution I made when I was here was, I succeeded in proving that...we believed that the reciphering process was literal additives and we thought it would be like the military additive which was 100 groups on a page. In actual fact, it turned out to be 80 five-letter groups and not 100 four-letter groups. That was my only contribution until I got home. But I was the first person who read Japanese into it. The...am I talking the right ~~subject~~ sort of thing?

Schorreck: Um hum.

Tiltman: For the obvious purpose of spreading the material over the additives, they tailed messages one after another rigorously through the additive. That means to say that if a group ended... if a message ended on the 26th group on page 59, the next message would start with the 27th group and so on, and I found ~~on~~ one particular lane, a great deal of material which actually went around the current table five times and I broke into it on the depth that was obtained by then and much to my surprise and everybody else's, it didn't come out in Japanese...it came out in Russian. It turned out to be somebody sending back recoveries in a five-figure Russian codebook. The...

Schorreck: This was the Japanese sending back their recoveries of a Russian codebook?

Tiltman: Yes... I'll finish the story for what it's worth...

Schorreck: Yeah.

Tiltman: This, as I say, was a literal additive and the codebook was digraphic - 2 letters, and it seemed to me that there was evidence that it was, can't think of the word, that the 2-letter groups were based on plain language. The numbers were arranged to the digraphs for numbers, were symetrically arranged in a diagonal across the chart, across the substitution chart, and it was possible to pick up in depth the numbers which because of this symetrical arrangement, you could see the difference between them was constant and so on. The messages, when they came out, they had 5 digraphs representing numbers, followed by a Russian word which was an identification of the...and then five more digraphs, then another Russian word and so on. The Russian codebook was one time, was one part, so that they were all connected alphabetically and so on. But, in every message they employed bi-section, that means to say, they cut each message roughly in half - the text of each message roughly in half and put the second half first. But there was one patch which was obviously the true beginning of the message, which was the only place where there could be any Japanese. This read in every case, "UF XI HN EI YR UF". This was the only place there could be any Japanese, and it had to be some kind of an address or signature.

"UF" was obviously some kind of a warning, saying, "This is the sender."; "XI", I read to be "DAI"; "HN", I read to be "HON"; "EI", I read to be "EI"; "YR", I read to be "YORI", which is from. It seemed that what we were dealing with was, "DAI HON EI YORI", which had to be the sender. I asked my...I was never a Japanese scholar... I asked my Japanese speaking friends in the office, "Who could possibly be calling himself DAI HON EI?". They were delighted...they said, "Oh this must be the General Staff Office, attached to Hitler's headquarters in Russia.". But it turned out to be not so. "XI" was not "DAI", it was "ZAI", which meant "district"; "HN" wasn't "HON", it was "Hungary"; "EI", for some reason was "BUKAN", which means "office"... and the whole thing represented...rested on the fact that I guessed that "YR" meant "YORI", which was from...it was just one of those silly misunderstandings. We read a very, very great deal of the Japanese military attache.

Schorreck: At this period?

Tiltman: Right through...right through.

Goodman: That's interesting. Would you comment on their cryptographic system and the Japanese Military Attache system as to its...it must not have been too secure, or was it a difficult system?

Tiltman: It was over used, like all these things...like our additives, our fleet general ciphers at the beginning of the war, which had such disastrous consequences in the battle of the Atlantic, convoys and so on. We tried to keep the Navy supplied with sufficient additives, but they were just over used, and the Germans read an enormous amount, but that's another story.

Goodman: That's what I was going to ask you...At this time period did you have any cryptographic responsibilities?

Tiltman: Yes.

Goodman: Would you tell us what they were?

Tiltman: From the time when Sir Edward Travis took over the office, which was in very early '42, I became officially Chief Cryptographer. This was only a name, but it meant that I was not only responsible for ciphers that were not being read, but I was also technically responsible for the security of all British ciphers.

Goodman: All British ciphers?

Tiltman: All British ciphers. I was the last word on security. I attended a meeting in the Admiralty once a week on Wednesdays, and mostly they were talking about distribution problems and so on, which weren't my business. But I was brought in, in every case where there was a technical point involved, and I was asked to try and cope with this bad situation in the British Navy. I should say that we had a good rotor machine (Typex machine), but we didn't have nearly enough to go around the Navy; so that what was required was a secure cipher that could be used by 1700 holders, all of whom had to be in a position to communicate with one another in cipher, and it had to be safe. It took a long time to introduce, but I did devise the SS Frame, which solved the problem. From the time it was introduced, which wasn't until the end of '43, the Germans never read another letter.

Goodman: From the Typex?

Tiltman: No. We hadn't gotten enough Typex to go around. What I mean is, that the solution to our COMSEC problem, we couldn't invent new machines or produce new machines in time to be of any use during the war, so that we had to stick to hand ciphers when you were fairly well equipped with machines.

Goodman: Did you have a responsibility for diplomatic ciphers and codes and ciphers as well?

Tiltman: Yes.

Schorreck: What kind of an organization did you have to do all this?

Tiltman: I had a private army of 12 people, headed by my beloved friend, the one who I wrote to yesterday...sorry, my memory is terrible this morning...J. Morgan, Dr. Morgan (he's retired many years, now). I had this research section which was entirely at my disposal and we had to handle all the...anything where anybody was stuck.

Schorreck: I think I'm going to ~~read~~ leave that COMSEC section for today.

Tiltman: Yes.

Schorreck: For the war period.

Tiltman: Yes.

Schorreck: That's amazing!

Could I get back and ask you one final question about this early period? If I could.

Tiltman: When you were talking...just a ~~minute~~ moment...when you were talking just now, you asked me if I was responsible for diplomatic... you mean our diplomatic?

Schorreck: Your diplomatic - British.

Tiltman: Oh yes, and it got as far as the Ministry of Food and everybody else eventually. I remember ~~one~~ the meeting in the Admiralty...the table got longer and longer and there were more people attached to it, and one day I went to my ordinary Wednesday meeting, and there was some kind of bombing activity going on. I was talking, and quite suddenly, I found myself alone in the room. Everybody was under the table. They were all used to the V-1 bombs and I hadn't come into...they knew that when one came near, when it would cut out and was liable to drop on top of us straightaway. I didn't know.

Goodman: It would have made your meeting smaller. (laugh)

Schorreck: Did you have any contact with Bertrand?

Tiltman: Yes, a great deal.

Schorreck: And what was the nature of that?

Tiltman: My memory is a bit thin...I met Bertrand first in May 1933. General Menzies took me over to Paris to talk to the French about what we were doing about Russian ciphers, and I flew over to Paris, and I spent one day with Bertrand and two other French officers. Bertrand, I had then met for the first time. I had very definite instructions that if I found the

French were unaware of Russian additive ciphers, and particularly the one-time pad, which had been introduced by then, I wasn't to talk about them. This was my first experience of Bertrand's intuition. He started off (he didn't speak English... ~~this~~ all had to be done through an interpretor, because my French wasn't good enough)...he started off by saying, "I realize that you probably have been instructed not to tell us everything you know, so we put down on paper everything we knew about Russian ciphers.", which made it easy for me. This is typical of Bertrand. So I spent the one day with him in 1933, talking about Russian ciphers and then not again. I suppose that I must have seen him in England in 1939, but you see, at the beginning of 1939, when the Enigma story was started, when the French were feeling out towards handing over what they knew about the Enigma, I was in Hong Kong, so I wasn't in it in the first place. Then when we decided to send a party, the party that eventually really got the essential information about the Enigma and went to Warsaw in about June '39, I was back and I was supposed to go, and they sent Knox instead of me...Dennie Knox. I think it was probably, from A Anderson's point of view, the right decision. But actually it was rather a disaster because Knox was without exception the most tactless man in the world and there was nothing you could do to stop him, and he missed the most important part of the information which was given him and I think it put us back six months or something like that.

Goodman: What was that information?

Tiltman: This is the...I don't know much about the Enigma. This was something I didn't have to deal with. It...it...what used to be called the diagonal, that means to say, the input alphabet which had been assumed would either be random or would be typewriter order, QWER and so on, in fact was in the ABC order. Now he missed that and in fact, he said that it had been tried and that it wasn't so. But he was wrong. This is all third hand, of course, the Enigma was never my problem. As I understand it, the way in which they gave him the...gave Knox the wheel ~~patents~~ patterns of the current Enigma was...they set the machine at a particular place and then typed a succession of A's, a long long succession of A's, so that the thing could be worked out in that way.

Goodman: What was your general impression of Bertrand? Did he know what he was doing?

Tiltman: He was fantastically good on the pinching side. I don't know to this day how much he knew about ciphers. I read his book and he does give a complete detail of the make-up of a German Service Enigma.

Goodman: I'm not sure of the use of the word "pinching". Could you describe it?

Tiltman: Well, it's a spy ~~word~~ WORK, secret service ~~word~~ WORK, that sort of thing. You know It all comes in his book. While we're on this subject, you asked me what sort of a man he was. Very early in the war, when we sent the British Expeditionary Force to fight

in France, I put together a party of cryptanalysts under Geoff Evans, you know Geoff Evans, Major...I suppose he was retiring about the time you were in...who worked in French GHQ on low ~~lead~~ level ciphers. We also provided them with a liaison officer named MacFarlane, "Pinky" MacFarlane, who worked in their most secret office, I can't remember the name of it, and was the liaison on the Enigma. Now after the Germans attacked ~~Entou~~ into, oh one story...A typical interview with Bertrand, who as I said didn't know English, would be in Bill Dunderdale's office. Bill Dunderdale is the half English/half Russian...our representative in Paris of our secret service...I would be talking, Bertrand would be sitting on the edge of his chair opposite to me, and when he saw you about to ask a question that he couldn't answer, always he'd say, "ne pas demander". (laugh) He always knew what was going on. After the Germans attacked into France, I think it must have been about May the 14th 1940, I was in French GHQ, negotiating the return of our party and Bertrand said, "We value your party very much; we'd like to keep them, but you'd better get them out while you can", and they were evacuated through Bordeaux. He then said, "And please tell your chiefs in London that none of your secrets will get into enemy hands.". Now how he made such an impossible statement, I don't know, because there must have been a hundred French officers who knew what we were doing on the Enigma and everything else. But they never did get into enemy hands. That's why his book has always astonished me. It seemed to me to be completely out of keeping with my memory of him. He put so much

into his book.

Goodman: How about the Poles? Did you have any...

Tiltman: I didn't meet them. I think I probably...I wasn't introduced to their most secret station...I've forgotten the name of ~~him~~ it now, until about March 1940. I paid five visits to Paris. I think it was only on the third or fourth one that I went to their most secret place and I must admit, I suppose I met one or two of the Poles. As I say, the Enigma was...I had enough problems without that, and I was told that was something I didn't have to worry about. We had...about a fifth of our office was engaged in it...had it's own special staff and so on, and I had absolutely nothing to do with it.

Goodman: How was material handled at this time - Brigadier, Did the British have...obviously they did...the British had a classification system, but there wasn't any special handling of certian systems, was there? For instance, that didn't come.....

Tiltman: Nothing corresponding to what you call "compartmented"... compartments. I don't think so, no...I don't think so...I may be deceiving you where I don't remember.

Schorreck: Could you give us, Brigadier, a general description of some of the people with whom you worked in this early period, let's say the World War II....

Tiltman: Before the war?

Schorreck: Before the war.

Tiltman: Before the war, my experience was that the best pencil and paper cryptanalyst was Fetterlein, the Russian. He was getting very old - he died during the war. He was getting very old and, for instance, he didn't succeed over the early COMINTERN and so on, but he was very good. Most of the cryptanalysts, there used to be 15 who were known as seniors, this was a particular grade of civil servant in those days. Of them, I should say that there were four or five who might just as well not have been there, they were left over from World War I. There was Strachey, who was also getting old, but had done very good work. He had been in the Army party in Cork Street during the war. There was Knox, who had a tremendous reputation. I never understood what it was...he was always a complete disaster whenever I dealt with him, but most of them were linguists, who were breaking codebooks. There really wasn't a great deal of clear-cut cryptanalysis done, except by Fetterlein and myself and just one or two other people.

Schorreck: Were Foss and Alexander engaged in the business?

Tiltman: Foss came in after I came back from India, came back in about 1933 and he is a glorious case of how difficult it was to choose people. He came up in one of the selection boards that they had

for the civil service. He was, as far as I know, a Spanish scholar and he wasn't accepted and then a couple of people who were accepted fell out and Foss was taken on. He really was very good indeed up ~~to~~ Jul the war period. He did the original analysis of the commercial Enigma. He broke the, as far as I know, he did all the proper work towards breaking the Japanese Purple...uh Red Machine, not the Purple. In fact, he was extremely good and he developed a flair for the mathematical side as well, which he wasn't brought up to at all. And then, unfortunately, he was very ill in 1940 and he was never the same man again. He was working on the Japanese Purple Machine when he fell ill, so we never really had a proper go at it. Not that this really has any relevance, because in the case of the Purple Machine, it had inherited from the Red Machine this division into...of the alphabet into 20 consonants and 6 vowels, or a 20-ring and a 6-ring, whatever you'd like it... however you'd like to put it, and it was possible that we had succeeded in finding that in some places we could solve the 6-letter ring, the vowel ring and thus have some few leads into the rest of it, and as I understood it, the early solution in this country of the Purple Machine really rested on their having done this kind of work rather more than we did and then there was a long, I'm open to correction here...this is all hearsay, there was a long handout by the British, which was transmitted back in the Purple Machine to Japan. Several part ~~partners~~ message in fact, and it was possible there to read a certain

amount of it simply from the reading of the vowel ring, and I believe I'm right in saying that Mr. Friedman succeeded in winkling the original text out of your state department, where probably nobody else at the time had the prestige to do it. Friedman, to my knowledge, never claimed anything more than that. It was his influence that succeeded in getting a hold of this complete crib to these long messages to break them. Then of course, a great deal of build up which led to the Purple Machine being reconstructed and properly read by the Americans. I say that because this is something we wouldn't have been able to get and Foss' work...Foss' early work on the Japanese Purple was good, but he was ill and he _____ the wrong one.

Schorreck: How about Alexander?

Tiltman: I'll tell you in a minute. Winterbotham, in his book, obviously confuses Foss and Knox. It's not his only inaccuracy... he talks about a very tall, dark man, and so on and so on. He's obviously thinking of Foss, and he's talking about Billy Knox. Alexander...Alexander was a very important...a wonderful man in the office. He'd been a...I think he was a schoolmaster at Winchester. Then there's a big department store in London, John Lewis, and the old John Lewis had a great idea of using mathematicians to organize his...organize his department store, and Alexander was one of the people to take it on and we actually took Alexander from John Lewis. But he was one of the people who came that _____.

We had a course, just before the war, arranged by Denniston for a small number of fellows from Oxford and Cambridge, whom we had hoped to get in the event of war coming on, and I gave them a couple of lectures; I can't remember what I talked about, but Alexander was on that course and so was Turing. I didn't have anything very much to do with Alexander technically during the war. He was working mostly, in my memory, on the Naval Enigma, which I had nothing whatever to do with. He succeeded me as "H". I was the first "H" after the war, and Alexander succeeded me. I think he was likely to have been a very much better "H" than I was. He had this wonderful power of concentration which came out, of course, he was a very fine chess player. He and ~~John~~ Josh Cooper, who is head of the "S" section. Either of them could do something that I was never able to do... they could listen to somebody give a very complicated demonstration or read one and remember all of it. Now I haven't got that kind of concentration at all. I suppose that if you want to talk about genius, the only one we had who could have been called a genius ~~is~~ was Turing. He was a little more peculiar. I think he probably made a bigger contribution than Alexander. But Alexander must have been very very useful in the Enigma field during the war.

Schorreck: How about Frank Birch?

Tiltman: Frank Birch had been in...he was a history fellow at one of the Universities...I don't know which...and he had been one of the original staff of 40 ~~over me~~ in the Admiralty and when he was brought into the office, he was put in charge of the naval section and the naval section did succeed in keeping people out as far as possible from naval business, and I think he did a very good job. I had to do with him on one or two occasions, but not really a great deal until after the war, when he organized our history.

Goodman: I have a feeling that the navy section, or the naval section...

Tiltman: The naval section before the war was terrible. There was a man named Clark there who knew every ship in the world, but had absolutely no idea of the technical side of our business at all. And wasn't a very strong personality; he just had this knowledge of naval matters that ~~we~~ _____.

Goodman: But they seemed to operate completely independently of everyone else.

Tiltman: They did, yes.

Goodman: Without any controls, so to speak...

Tiltman: Yes, they were a little bit out of control.

Goodman: Was that because of Denniston's.....

Tiltman: No, I think it was chiefly Frank Birch's doing.

Schorreck: Were there any other names that you can think of, Brigadier, that we should be familiar with from this early period? Prior to the war, although I know some of these went on through?

Tiltman: We had a very famous lady, Emily Anderson, who wrote the standard books, The Letters of Beethoven and The Letters of Mozart. And I never worked with her, but the story was that she once ~~was in~~ got into an argument with Denniston, and she said, "You don't seem to understand, Commander Denniston, that my work starts when I leave your office.". She was very good. She lasted through the war. She was in Cairo for a bit.

Schorreck: She was a cryptanalyst?

Tiltman: Yes, in the old standard codebook and additive period.

Goodman: Who was producing British COMSEC materials at that point, in that early period? Did you have anything to do with that? With the sections?

Tiltman: What I did, I did on my own authority, my own thinking. I...you probably know from having read my stuff ~~that~~ about the SS frame, which solved the general fleet cipher...well, I devised the first grille additives, that is to say an additive ~~with~~ in which certain groups appeared in windows on a sheet. In 1933, I made a cylindrical device, a very elaborate one that could be changed fundamentally by a memorizable codeword, but I was quite unpopular... cryptanalysts weren't supposed to invent ciphers and I was told to keep off it. But it was useful to me later because in I suppose late in 1940, I was called in to examine the ciphers being used by the free Poles, who had a headquarters in London and they were using sheets of 4-figure additives and I suggested then that they should put masks on these with windows and so on. So that I had it in my mind when the problem of naval

cryptographic security cropped up in 1941, when it was put to me.

Goodman: As you ~~well~~ know, there was an extraordinary outpouring of COMSEC materials ~~through~~ with the war, and I wondered what their antecedents were if, in fact, there were joint ciphers used between the British forces, who produced them, How were they contrived?

Tiltman: I do know that the War Office ~~used them in the war.~~ ones were made up in the War Office.

Goodman: In the War Office. So, everybody had their own individual responsibilities...by sections

Tiltman: Yes. Who, for instance, devised the Foreign Office ciphers, I simply don't know. As far as I know, they eventually... I don't know...they eventually got into one-time pads, but I don't remember much about it.

Schorreck: Many of the outstanding people in this business, in general, the 1930's and in the war itself, were people like Friedman, or like Frank Rowlett, or like Sinkov, or like yourself, and like Safford, who were involved in both sides of the activity, both cryptography and cryptanalysis.

Tiltman: Yes, it wasn't until the war that mine was anything except my own dreaming. I didn't have any responsibility.

Goodman: But wouldn't you think that this is a good idea?

Tiltman: I think it's a most excellent idea. I owe a great deal of my...any success ~~that~~ I've had in the way of diagnosis of ciphers to having had all through the years to think of the other end of the business.

Goodman: It's very obvious there was a great deal of technical interchange between the...what were initially the ~~cryptees~~ cryptees and the COMSECers and let that flow up. Is that kind of thing being done now?.....at all?

Tiltman: I don't know. I'm not in touch. I'm 20 years behind the times.

Goodman: You mentioned the Typex earlier on. Do you recall how that appeared on the scene? Did you have anything.....

Tiltman: Typex was, I think, ~~was~~ devised by a RAF Wing Commander named Lywood, which was simply the British development of the commercial Enigma machine.

Goodman: It was an adaptation?

Tiltman: An adaptation of the Enigma machine. It wasn't such a complete re-make as the ECM or the American one, but it was quite a good machine.

Goodman: I want to ask you something about this...You mentioned Winterbotham a minute ago...I'd like to clear up one point from your view. He makes the statement that the Japanese ~~invented~~ had and ~~the~~ Purple machines ~~are~~ of the Enigma family.

Tiltman: Oh yes, he didn't know what he was talking about.

Goodman: Oh, That answers the question.

Tiltman: He didn't know...he...I knew Winterbotham. I doubt that he ever, in spite of his being mixed up in the middle of it all the time, I doubt if he ever understood how either the Enigma machine or any of the machines ~~he~~ used to break it...He hadn't the slightest idea ~~of~~ how they worked. I've heard the expression that when he talks about the bronze goddess and that. I never heard the expression until I saw it in ~~the~~ his book.

Goodman: a lot of other people didn't either.

Tiltman: Winterbotham, as far as I know, ~~Winterbotham~~ did his own job very well. His own job, as far as our work is concerned, was that he was responsible for organizing the SLUs, the Special Liaison Units, which looked after the security of our results.

Schorreck: Disseminating that information.

Tiltman: Yes. As far as I know, he did that quite well. I don't know whether you've seen his latest book, about his work before the war when he was buddies with Hitler and Rosenberg, [illegible] and all the rest of them; he can't have invented it all, but I paid, during the COMINTERN time, I paid 3 visits to Berlin. On each occasion, I stayed with the head SIS man in Berlin and I never heard of ~~him~~ Winterbotham. I've no doubt, ~~So~~ as far as I know, it's all true. When he touches on our stuff, he's most unreliable...and could have been stopped.

Schorreck: I wonder if we could possibly touch on that question we were talking about a minute ago...about the transition. Is there a transition that a cryptanalyst has to make when he's dealing.....with machines?

Tiltman: All I was going to say was there are people who say that the breaking of the Tunny machine, that's the teleprinter machine, is the...I forget...Campaigne says that it's the best cryptanalysis performed in recent years...or whatever... I don't remember what he really does say, but I broke the...I produced the bit of key on which they read the thing, and I know nothing whatever about machinery. But it had to be reduced to paper terms for me to deal with it at all. That's all I was going to say. In the same way that the early work on the Enigma was done by paper methods before they invented scanning machinery. and so on There used to be a document called a Foss sheet. A Foss sheet was a large bit of paper with perforations in various places, which represented, I presume, what later they called a menu. You laid this down on a glass transparency with a light underneath. All these things, you see, they're not really bringing machinery into ~~it~~ the thing at all.

Schorreck: Is there any difference at all in your approach to cryptanalysis.....

Goodman: Machine versus ~~the~~ manual....

Schorreck: Machine versus ~~the~~ a manual produced system? Is there any approach ?

Tiltman: I'm too far out of date to answer that. I think that things have changed so much with the introduction of computers and so on, in which I have no part at all.

Goodman: Well, then perhaps we could go at it another way...

Tiltman: I don't know whether I'm even talking sense.

Goodman: Yes you are. If you could tell us, or could you tell us what sort of person you see is the one who makes the best cryptee, or who seems to do the most reasonable job?

Tiltman: That is an interesting point, because until the war broke out, it had never occurred to anybody in my office that mathematicians had anything to do with our business at all. As far as I know, the first pure mathematician taken on was in about 1938, when the war office succeeded at last in giving me two permanent civil servants. One was Dryden, the other one was Twinn. Dryden was a German scholar, Twinn was a pure mathematician. But I don't think they were taking him on consciously as a mathematician, but just as a highly qualified intelligent...

Goodman: All-around scholar, that sort of thing.

Tiltman: Yes. I had nothing to do with the introduction of scanning machinery, Hollerith machinery. To my shame, I have to admit that back in about 1934-1935, a man named Guy Liddell in the SIS, took me down and gave me a demonstration in Hollerith and I didn't understand at the time it's application

to our work. I had so little...well ~~by~~ then Sir Edward Travis introduced a rival form of the scanning machine into the office with one lady operator. This was Power's machinery. This was another way of doing the same thing that Hollerith did and I did a test and I found that I could beat her in time in an analysis job. This was a completely unfair test, of course, because the development of machinery is not dependent on one person pounding one machine which is what happened to her. She did all the punching and everything else. When we did take on Hollerith, it was done on Sir Edward Travis' responsibility and we approached it in a slightly different way, I think to you. We imported a whole Hollerith unit, which belonged to the Hollerith Company, under a man named Freeborn, who stayed with us until after the war.

Goodman: Could you talk to Sir Edward Travis' policy a moment ~~among~~ which you haven't described him at all?

Tiltman: This is a little embarassing. I crossed swords with ~~talked to~~ him many times. He was a good friend of mine. I knew him back to 1920, and I would rather not; I hadn't even in my papers for the British Office. I would rather not give a description of what I feel about Travis. He did a wonderful job for us during the war, but as far as I know, the most important part of it was that he maintained this high-level contact through Menzies (construct?) to the Prime Minister by which we got everything we wanted. We had so much priority; without which we couldn't have built up the vast

machinery for the Enigma and the Tunny that we did. And which I don't think Denniston could have done. Denniston was a very good man, but I don't think his thought was quite on that scale. So, I think I can say that Sir Edward Travis...that he did a wonderful job on that line. ~~Other~~ Further than that, I'd rather not ~~bear it~~ go Not without thinking. You mentioned DeGrey...DeGrey became Travis' deputy during the war. He was a ~~very~~ clever little man, and one beautiful function that he produced...that he had was that, when Travis was abroad, over here for instance, DeGrey's way of dealing with the problems of the office ~~were~~ was....How would Travis do it? And that's the way he did it, so he was almost the perfect deputy. Whether people liked his decisions or not, he was Travis when Travis was away.

Schorreck: That was Nigel DeGrey?

Tiltman: Nigel DeGrey. There are four from the beginning of '42, ~~who~~ there were four deputy directors. I was DD-4, DD-2... DD-1 was DeGrey, DD-2 was a Naval Captain named Bradshaw, who was the head of administration, DD-3 was Captain Hastings (I don't quite remember what his job was ~~at~~ in that stage), DD-4 was myself.

Goodman: Did Mr. DeGrey and Sir Edward have any sort of technical background with respect to codes and ciphers, and so on?

Tiltman: DeGrey had been...Travis was...came into the office as a serving paymaster Commander. He was really sort of on the COMSEC side and he was representative of the Admiralty in our office. And, how he came to be deputy to Denniston, I don't know. And took his place ~~from the office~~ when the office got very large.

Schorreck: (Sir,) I wanted to ask you a kind of a general question. Somebody, I think it was Kahn, made a statement that there was only one cryptographic system that had ever been broken by pure cryptanalytic effort as opposed to having been, part of it being captured or codebooked, or captured and recovered, pinched or stolen, or filmed, or....

Tiltman: That, of course, is quite untrue. The ideal case is Tunny. We had absolutely no information at all except the early intercepts which were brought to me by Kenworthy. Kenworthy was the head of our war office wireless service, and he had picked up the early Tunny intercepts on search and he brought them straight to me in bulk and put them on my table. We tried to get some collateral information, but I couldn't get any at all. It was purely and entirely cryptanalytic work. I'm absolutely certain of my facts there No hint...

Schorreck: I can't believe there weren't others as well that were reconstructed from absolutely nothing.

Tiltman: Oh yeah, it's not...it's just not true. Kahn, Kahn doesn't know the stuff there. He knows a great deal more than he did when he wrote the book....Been here. I spoke to him once on the telephone. He rang me up and said that everybody told him to do it. He wrote me a letter first saying everybody thought I was the top technical man in this country and that later on he would give me a call, and when we had a call, and it made me very angry because he simply would not understand my security point of view. He didn't understand that I did not wish to be

connected in the public eye with his work at all. Then I never had anything to do with him again until he wrote to me two years ago and asked me for a copy of ~~an~~ my off-print of my paper on the Voynich manuscript which I was very glad to send to him. I wrote a nice letter back to him, saying this is the best he had read on the subject. So, we're not enemies.

Goodman: But you're not friends either...I think until the next time he can figure a way to use you.

Tiltman: But, I have nothing against Kahn. He never was in the office. He was a journalist who specialized in this subject and got interested in it.

Goodman: Very aggressive.

Tiltman: Very agressive, very aggressive, I quite agree, but I put him in a different category altogether to a man like Winterbotham. I would have said to Winterbotham, and this is only hindsight...our director had a long time to do it because we negotiated with Winterbotham for a long time and we tried to get legal action taken against him under the official Secrets Act, which was defeated because we were advised that we would never get a case through to him unless we could prove he was doing damage to our security now. I would also have said to Winterbotham, "You are a regular officer, you are a regular officer. We'd like you to know that your colleagues regard your actions as being dishonorable.". I don't believe he would have taken that. The damage he's done is not by anything he's disclosed, but by the fact that ever since he's written

that book, everybody...Tom, Dick, and Harry thinks they can write what they like ~~without our~~ and not ask permission.

Schorreck: And the problem with Kahn is that since he is so technical, that even Winterbotham admits that he uses Kahn as a technical source and in technical matters, Kahn may not know and often does not know what he is talking about. And so that kind of thing gets perpetuated.

Tiltman: No, he doesn't know. He picked it up in bits... he picked it up in bits. He's a clever fellow...he's picked it up in bits. Neither he not anybody when they talk about it, or the man who has just written the book, The Man Who Broke Purple, have any conception of what the ~~book should be~~ machines were like...they didn't know what the essential ~~factor~~ character of it was...or how to ~~write~~ it was broken, and they never found out.

Goodman: Could you...you mentioned Mr. Kenworthy a little bit earlier today as head of the war deptartment inter...

Tiltman: Not war department.

Goodman: I'm sorry, the war office intercept.

Tiltman: I don't think he was war office. Kenworthy was a civilian, I don't suppose he ever belonged to anybody except the Foreign Office. He was a very good hand operator, very good hand operator.

Goodman: You suggested that he brought you the traffic.

Tiltman: He picked it up himself on search. It was in the days when the good old-time operators went out on search. The other man who was wonderful was Lambert, who was the man in our office who was responsible for wireless interception.

Goodman: Could you give a time for that or a date? Was it 1930.....

Tiltman: Well, I can go back to 1933, when Kenworthy and Lambert set ~~off~~ out with their own truck to try and trace the COMINTERN agent who was operating from London.

Goodman: Well, I'll be durned.

Tiltman: They got the house next door. (laugh) But an intercept by Lambert...Lambert on his own after hours would listen to the COMINTERN, and the handwritten intercept by Lambert was the most beautiful thing I ever saw at the time. Lambert was very famous for another reason. Under the name of A. J. Alan, he used to telephone his stories on the British Broadcasting and they made a great thing of keeping his identity secret, they suceeded...they suceeded in doing so. He was very, very famous, a storyteller. He died during the war, too.

Schorreck: That's all I have.

Goodman: That's a good place to stop, General.

Tiltman: All right.