Note: This is a transcription of one of the tapes of SCAMP talks (Lecture "F") set. Destroy

All right, let's turn the lights out and ring the bell, I think there is some absentees here.

Well, let's go on with the slides. There are a couple of slides Iwant to show. I am going to talk a bit about the traffic analysis from our own point of view of communication security. This is meant to illustrate the important intelligence that is derived by traffic analysis by watching the flow mfx and ebb of traffic and this one shows convoys across the Atlantic from Hampton Roads and Algiers. The chart shows the daily breakdown by security classification of the traffic from Hampton Roads, Port of Embarkation, to Algiers, North Africa for the month of April 1944. Three definite peaks in traffic volume are evident, each of which indicates a convoy movement from Hampton Roads to Algiers. The approximate size of the movement is judged from the total messages in groups and peak periods while the destination and route are given away by addressee callsigns in the messages. Close inspection will show that the first traffic search began on 4 April, the second on 13 April and the last on 22 April. Experience has shown that these traffic peaks appear on the circuit the day or two following the actual convoy sailing date. The convoy movements are therefore called on the 2nd, 11th and 20th of April. Furthermore, the traffic study shows definitely the proportions of supplies and troops carried in each convoy. This is due to the fact that all passenger messages are classified secret, cargo messages are classified confidential. Detailed analysis shows that there were 21,836 confidential groups and 3,965 secret groups transmitted in connection with the 2nd of April convoy. The next convoy gave rise to 18,160 confidential and 4,470 secret. The third convoy

required 19,429 confidential and 594 secret. It is apparent from these figures that the major function of each of these convoys was to carry equipment and supplies.

Well, you all remember I am sure the various signs that were posted in buildings -- Keep quiet, the enemy is listening and Troop movements are very very guarded. Now I am going to read you from a book with the strange title, "All Honorable Men" by James Stewart Martin, who apparently was a member of some OSS or Economic Bureau or one of the War time economic things of the government.

"On a bleak night in February 1945, I found myself standing with my small party of investigators in mist at the Washington airport waiting to take off. As I stood in the gloom observing all the security measures that surrounded our routine departure, the black out of the field and planes, silence and sudden orders, I remembered our discovery earlier in the war of how easy the secrecy of ship sailing had been penetrated by the Germans. In 1940, 41 and 42 ships leaving American seaports had had the same security measures to protect their departures yet many of their broken hulls and water-soaked cargoes had washed up on to the beaches of New Jersey, Virginia and the Carolinas where German submarines had spotted them with in sight of shore. In case after case, every man on board had been marked before the Captain opened his orders. No they may not have known it, the cargoes they carried were reinsured with Munich. The routine system of placing insurance had put precise ~~intercept~~ information on their sailing date and destination in the hands of the Germans before the

ship left port. In the summer of 1941, before there was any economic warfare section, several trustbusters discovered that while the American public was looking more and more askance at German business connections, insurance companies doing an international business seemed to have no such doubts about their foreign commitments. Insurers of large risks, such as ships, cargoes and industrial plants, customarily spread the risk among other companies willing to take fractional shares. The big insurance and re-insurance companies in the United States which handled the largest risks have such treaties on an international basis through arrangements with the Lloyds group in England or with the Zurich group in Switzerland. It had long been the custom the American companies to place their reinsurance on ships and cargoes with the Zurich group by cabling information to them so they could accept responsibility for a share of the American insurers' risk. The information cabled would include the name of the ship, the sailing date, the cargo carried, the destination and the value of the insured property. One detail which should have raised someone's eyebrow but did not until the government stepped in was the fact that the Zurich group in turn had a reinsurance treaty with a Munich reinsurance pool in Germany. The result was that during 1940 and early 1941, by the time a ship had cleared New York or Baltimore harbor, headed for a European port, the German intelligence service already had the sailing date in hand." This goes on to tell about how anyone who was interested in some of our big buildings could purchase blueprints for $.50--for $.55 he had the plans of the White House showing the locations of the fire extinguishers and other protective apparatus. For $.75 he had the plans for a

new large magnesium plant, one of the blueprints had an arrow pointing to a valve with a legend--under no circumstances must this valve be closed while the plant is in operation as an explosion would result. So much for our protective measures from messages. It's just almost impossible to tighten up everything apparently.

Well, now, let's see what the next slide is. I am going to pass that up. That's some more traffic analysis and I am going to devote the rest of the talk to cryptanalysis. The most important steps. First, the study of external characteristics of messages. Second, study any available collateral including that obtained from previous solution, this means cryptanalytic continuity, very important. Study the beginnings and ends of messages. Search for repetitions between and within messages, preparation of statistical counts of letters, groups and etc. Search for indicators, determine the type of cryptosystem used, separate the traffic into groups of messages in the same or related keys, test for probable words, stereotypes and algaes, isologs, homologs. Then reduce it to simplest terms.

The rest of my talk will be devoted to a brief discussion of modern, practical cryptanalytic techniques and gadgetry. Now we turn first to a picture of an old gentleman, Trithemius, whom I mentioned earlier. His picture matches the one that the average layman has of a cryptanalyst. The curtain of secrecy has imparted an air of mystery, and before World War II, it was possible to do much COMINT processing merely with pencil and paper, sliding strips, and simple aids. Now cryptanalytic work is big business, complex and very expensive, but it pays big dividends. ~~You heard Dr. Engstrom say that~~ at the present time we are spending about a half a billion dollars a year on this

activity. Now the cryptanalysis in modern systems has been facilitated by the invention, development and application of special cryptanalytic aides by way of machines. The nature of the problem, not merely the number of permutations and combinations but the type is more important. The nature of the problem is one of testing out the multiplicity of assumptions and hypotheses, commonly by statistical methods. I'll show you a picture of what I think is the earliest cryptanalytic device, one that I made at Riverbank in 1915 or 16. Sliding strips between two glass plates, I can slide them easily, they are in tracks and rubber rollers so I could print alphabets fast, single alphabet or a whole row of alphabets--the polyalphabet. In 1934, I became quite chagrined that we didn't have any kind of machine apparatus to help us and the Navy did. I found this out by secret channels. The Navy began in 1932, if I remember correctly, with one IBM SET, a punch, tabulator, sorter and they used it for cryptanalytic purposes and there came a time then a couple of years later when I found out that there was a possibility that we could get some. There was no hope that we could convince the Signal Corps people that we should put in our appropriation for this thing so there came a time when I found out that in the office of the Quartermaster General of the Army, there was an installation -- a sorter, a punch, a tabulator and that a new officer had come to take charge of this particular division . The division had to do with the accounting for the CCC, remember that gentlemen. This officer didn't find that Henry Bennett who was Quartermaster General to George Washington used machinery so he decided that he would have this taken out so when I found this out, I maneuvered to get

the remaining term of the contract transferred to the Office of the Chief Signal Officer and that was done by a memorandum--you can see blood and tears on it -- which I wrote putting my case forward in my own handwriting, what we could do if we had a little help of that sort and this is the extract of the first contract that we actually got with IBM for our apparatus. From that small beginning I show you now one wing of a big building at Arlington Hall during World War II which contained nothing but IBM machinery and we had two such wings. They were several hundred feet in length, hundreds of machines.

Now I would like very much to be able to show you the examples of the two most important machines that contributed to the cryptanalytic victory in World War II but I cannot. These pictures would show you a Navy type of bombe, a word which we took over from the British, who took it over from the French, who took it over from the Dutch (I think it was the Dutch). The Navy had a different type of machine from the army. They went in for high-speed commutator devices, if I remember correctly, the rotational speed of the commitators is 18,000 per second, 18000 revolutions per second, this is a very high speed thing and they were going to have at first 336 of these machines, each machine having four commutators. The reason for the four is that the Naval Enigma had four rotors and the reason for the 336 is that the set of rotorsthat they provided for Naval use, there were 336 permutationsof the rotors that could be used in one date or in one period--twelve hour period. The Army went in for electrical relay solution machines which we installed in a big wing, basement wing of Arlington Hall. It was a tremendous thing built for us by the Western Electric Company and we called

her Madame X. It's impossible to show you a picture of that thing because it was much too big to get into a picture but I don't have a picture of the Navy bombe, I wish I had. I don't know whether the Navy even had any pictures of the bombe taken. It may not be too late. I think the Navy has one or two still in operation.

Now we are going to come to the specialized types of machines which both Services use. I can show you only pictures of those specialized types that Army used because I happen to have them. I don't know whether the Navy had any pictures taken. This is something I will have to inquire about--I got these together for the talk. I am sure however that they had as many and as complicated, if not more complicated, machines than the Army had. I must say one word about a machine which the Navy designed and I don't know whether they actually built it or not, called Duanne, toward the end of the war. The solution of the enigma depended upon one thing, two things really. First, no change in the wiring of the rotors/and secondly, the possession of a crib. That is, the knowledge, the Germans didn't do this throughout the war pretty definite assurance that a message would have a certain word or expression in it. Without that you couldn't even start. We didn't have any trouble getting these cribs because of the methodicalness of the German minds, I mentioned that before, so that there were always cribs available and you would be astonished at the sources of some of them. For example, the solution of messages to and from Rummel would be dependent upon catching a crib of some lonely operator way off the coast of Norway who was reporting, "nothing to report." On some of these crib sources, the British and ourselves had double and triple coverage to be sure that every letter was taken. It was that important.

Now we have to have machines to make coincidence counts of in comparing messages. If you have a message of 200 letters and you want to compare it with another message with say 200 letters to see if they are by chance the same cipher or whether they are slid, displaced a little bit. You can do this by hand, yes, one person can do this sort of testing, comparison, about one comparison a second but that would take for 200 messages which would require about 40,000 comparisons, they would take about ten hours. This is much too slow so we built a machine to make the comparisons and we call them comparators. We have machines now at NSA, one a ROBIN will make 50,000 comparisons a second. We are going to have a machine if it already hasn't been made and built, the DELLA, I think it has been delivered, 5 million comparisons a second. Now this is many times the capacity of ROBIN and you can see what effect machines of that speed would have upon cryptanalytic techniques in the future. The first comparator that was built, I mean a real sort of a job, was the one built by Vannevar Bush at MIT for the Navy. It was a 70 mm comparator but we had in Army breadboard things that we used for several years before the Navy's comparator was put out.

Now I'm going to show you some pictures of some of the types of machines and I'm going to say just a few words about each of them perhaps.

First I'm going to show you ALCATRAZ--that's the ALCATRAZ, we just passed it. ALCATRAZ is a machine which will make monographic and diagraphic frequency counts, columnar, or anyway you please. It was a great big thing, very bulky

and we have better ones now.

Now this picture shows you an automatic deciphering machine. I don't know what the caption I think that deals with the Japanese Military Attache.

Here is a machine which will locate repetition between messages and we call this a BRUTE FORCE machine because we don't make any attempt to do a first sifting. You take all the messages and just push them through the machine and hope that you are going to find a repetition. That's a BRUTE FORCE machine.

Here's another one, called the SLIDE RUN machine where you have a displacement of the messages. You want to find where they should be superimposed.

Here is a machine for decoding and deciphering--I don't know now just what it was, it was a war-time machine.

Here's one which was called the CAMEL that was a machine for locating certain types of indicators in Japanese military traffic.

And this was the CAMEL CODE INDICATOR-LOCATOR and a specialized thing also for the Japanese Army ciphers.

Here is a machine ~~with~~ which consists of an assembly of components, some special job, nothing complicated about that but just getting together the necessary number of parts for the particular job. And sometimes these things had to be done in a hurry.

This is a machine which was used for a system called JAS and I think that was Military Attache system? I forget, but anyway that was one of the machines

that was used. Oh, that's an Army Ground Force.

This next one is Selective J-Square. You remember that square that I showed you, it looked like a magic square, they had a number of those in simultaneous use and this machine was designed to pick out which one was used for a particular group of messages.

Next is a J-Square permutator. The same sort of thing. You had a plug-board here and you could plug in to see how many plugs there were. I think the back of the machine shows a little complicated wiring that had to be undertaken.

This is called the PURPLE DUD-BUSTER. In connection with the PURPLE machine, we had many times messages that had garbles in them and it was important to try to get out every message and to degarble by hand, which was kind of difficult and a slow process, so machines were devised to locate and to eliminate the busts as they were called or duds.

This is the GEE. That's a German one-time pad system about which I told you. This was the machine that was used to generate that additive. I am sure it didn't look anything like the original German machine.

The next is the GEHEIMSCHREIBER CRIB TESTER. If you had some crib that you wanted to try out on one of the fish systems, this was the machine that could help you.

This is what we called an AUTO-SCRITCHER. That is what the boys called it, I called it RODAN, because in a way it was a thinking machine. It didn't do things quite by the exhaustion method--it would take a hypothesis, go through a certain number of steps testing and if it got to a contradiction, it would

say, "no, it's no good, go back again, young man", and this it would do time after time until it got a hypothesis without contradiction and that then led to the solution of the particular ENIGMA key.

Here is a machine called O'MALLEY. It was a specialized arithmetical computer. It gives the summations of products of pairs of numbers.

Here is DEMON II which is a high-speed type of comparator thing and next we have GOLDBERG which is the first general purpose large-scale coincidence machine. This is the first machine that NSA had built with the magnetic drum for storage. I think there is another picture of GOLDBERG--you can see the drum over on the left peeking through the aperature there.

And, of course, we had ATLAS. This is ATLAS I, we had two ATLAS II's and these, of course, were replaced by the more modern digital computer machines, specialized 7#1's and other types of machines. And we are going up to, you heard what Dr. Engstrom said, higher and higher speeds all the time.

Now I had hoped to show you some slides or a beautiful chart which depicts the story of the battle of the Atlantic--a most stupendous, fascinating tale, stranger than fiction. The story of the Battle of the Atlantic has remained a profound secret. The Germans are very smart people but they lack imagination. The Germans knew that the enigmas could be solved. They had worked out on paper methods for solution, mathematical demonstrations and so on, but they said it was impractical--couldn't be done, it would take forever to reach a solution. It never dawned on them that one could build machinery to do what they thought had to be done by hand. That was a fatal failure, their

imagination. Now in the Battle of the Atlantic, the Germans came to a time when they felt there is something strange about how their submarines meet up with Allied ships, way out of the way. How is it? Well, their ciphers were secure, this they knew, so it couldn't be ciphers. It must be treachery, it must be spies. What did they do? They adopted the practice of not giving the Captain of a submarine his sailing orders sealed in an envelope as is often the case but they told him to go to sea and they would send him word. This was a very fortunate thing for us because then we had the envelope open and the failure of their imagination, their methodical minds, their addiction to sterotyped messages caused their downfall. Now the funny part of it is too that they tried to account for the submarine losses in another way besides treachery. It must be direction finding. The Allies must have some very high-powered new kinds of direction finding gear and do you know, strange to relate, the books that are coming out of Germany even today, describe their loss of the Battle of the Atlantic to high-powered radar direction finding and that sort of thing. It hasn't dawned on them that if that were the case, if there were such a thing as high-powered D/F, high-powered radar apparatus in 1943 when they began losing submarines by the scores, surely the art would now have something to say in the periodicals but, no, their imagination has stuntified their thinking and it is still ascribed to direction finding and radar. Let's hope that they continue in this delusion. So what I have been telling you is a profound secret. I mention to you that in a talk which Admiral Wenger gave before the Navy War College he deliberately misled them,

the secret is so precious. I want to take this opportunity also to say that this country owes an enormous debt of gratitude to the brillance with which Admiral Wenger and his superior, the Director of Naval Communications, Joseph Redman, operated this precious communication intelligence source during World War II and the Battle of the Atlantic in a manner that left no leakage. It was a brilliant execution of security arrangements. The submarine commanders who were told to go where, the destroyer commanders who were told to go where, had no idea and weren't told so the precious secret has been kept. The slides I tried but they are too dense, they don't show and it's a beautiful story to tell but I will have to pass it up.

Now, in the Pacific Theater-- I have already indicated to you some of the principal reasons for success on the failure on the part of the Germans but I must not fail to mention that we owe a tremendous debt to our British Allies who showed the way in the enigma and in many of the other systems used by the Germans and the Italians. What we gave them were Japanese systems in exchange but their contribution to assist America is incalculable. Besides the things I have mentioned on the part of the Germans, lack of imagination, in the Pacific, there was lack of technical know-how. The Japanese mind piled complexity on complexity thinking that this is what will kk give them security. They made many errors in their complex systems--they couldn't help it. I wish I could show you their machine for producing their random additive groups. Gentlemen, it's pitiful, pitiful what this intelligent people did in this line. Their machine for making random additive pages number because their systems were

so slow and so complicated and so open to attack, we read pretty nearly everything.

Besides the failures on the part of the Germans, the Japanese, and the Italians, and by the way, Dr. Hall has reminded me that the Italians did use the Hagelin machine in their part of the war and I think it was the British who read most of the traffic, besides their failures in imagination, don't forget that there was brilliance on the part of the Americans and British cryptanalytic staffs, I will except except present company, and one other thing, very important--lots of money, millions of dollars.. Without the money, I don't think we could have done what we did. The last few charts I think might be interesting. Let's see for a moment--to give you an idea of how

and finally winds up by courier to the Pentagon. We didn't have really just the couriers, we had telegraph teletype lines, secure lines with crypto gadgetry on them.

This is a chart which shows the production of decrypts for the period 1 December 1941 through ~~December~~ 31 August 1945

over 11[illegible] messages and this is the cream of the crop--there were only translations made of the ones that showed some useful information. This is the Navy distribution system, the way they linked up their various comint operating centers, complicated, controlled from the center in Washington. And this is a picture of the combined Naval-COMINT organization. There were various centers in the British centers.

Now I think we can stop the lantern slide and I am going to talk for the next few minutes some more about what it meant and I will read some extracts from a report of a committee, appointed by the President in 1952, to look into the cryptanalytic activities of the United States. There was a bit of unhappiness about the way in which the Army and the Navy cryptanalytic organizations had coalesced. Some people thought it was a shotgun shot gun marriage, perhaps it was. There was a desperate desire to make it work and in order to make it work better than it had been, the President appointed this committee, headed by a New York lawyer who had had some experience in this business during the war and they studied the case and they brought in a report with recommendations for strengthening the Armed Forces Security Agency, as it was called on its first union, and I will read from that report because it had some -- this tells the essence of what was done during the war.

"In World War II, COMINT may well have been our best paying investment. Its cost cannot be accurately computed but an informed guess would be perhaps one-half billion dollars annually. General Handy is reported to have said that it shortened the war in Europe by at least a year. In the Pacific COMINT located the Japanese Fleet enroute to the Coral Sea and again enroute to Midway in 1942 enabling us to mass the carriers for the battles which generally are regarded as the turning point of the war against Japan."

An extract from the report of the Joint Combat Intelligence Center, Pacific Ocean areas on this engagement reads as follows: (and this is in the Brownell Report).

"The factors that vitally affected the Battle of Midway ~~xxx~~ were many and complex but it is undoubtedly true that without radio intelligence, that is COMINT, it would have been impossible to have achieved the concentration of forces and tactical surprise that made the victory possible. In 1942 COMINT told of the critical Japanese decision not to join the Axis war on Russia." The funny part of this is, the U.S. authorities thought this message was a phony meant to deceive us. "In 1944 it helped us to pick the soft ~~xxxxxxx~~ spots for our island advance ~~xx~~ often showing us where the Japanese expected us to attack and where their troops were massed. The strategic bombing survey mission which checked on shipping losses after the surrender discovered that COMINT's knowledge of the size and location of the Japanese Merchant Fleet on V-J Day had been more exact than the records of the Japanese ~~xxxxxx~~ Ministry of Merchant Marine/itself. COMINT provided us with our only reliable measure of how fast the Japanese were losing their will to resist. Our leaders had an immediate and thorough record of the peace feelers which the Japanese asked Ambassador ~~Satow~~ Sato, in ~~Mexico~~, in Moscow, to send us through the Russians and of the explantations to him of how decisions were being reached and on what points further concessions would be made. In connection with this, the Brownell Report doesn't tell us, but you see we were reading these peace overtures of the Japanese, trying to

to get Moscow to intervene, ~~xxxxxxx~~ to call a halt and Satu was in touch with the Russian Foreign Office and we set back and waited to see if the Russians would tell us about these peace feelers. Not one word. The principal credit for winning the Battle of Britain has gone to radar in the public eye, and the so few to whom so many owed so much, but much credit is also due to another British few who rapidly deciphered the high level combat traffic of ~~Luftwaffe~~ Luftwaffe and guided the airborne few to the defense of the right place at the right time. In ~~North~~ Africa COMINT did even better. It read Rommel's intentions ~~in Africa~~ so well that the desert fox guessed the truth. He confided his suspicions to Berlin, only to be told by the German High Command that such things were not possible.

Before D-Day in France, COMINT furnished periodic appraisals of the situation for the High Command showing where he felt the main attack would come as well as some of Berlin's replies ignoring good advice presumably in favor of Hitler's intuition.

COMINT also contributed Ambassador Oshima's detailed reports to Tokyo on his pre-invasion tour of the channel defenses which led to basic revision of our landing plans. After the assault was launched, COMINT supplied a large quantity of battle reports, battle orders on every level from the OKW itself down to the various divisions.

Throughout the campaign in France and Germany, our estimates of enemy troop strengths location and intentions were based more on COMINT than on any other source.

COMINT WAS also the principal source of information used to select strategic and tactical bombing targets ~~anyang~~ behind German lines and it helped us to identify the testing of advanced weapons, such as improved torpedoes and guided missiles, in time to get our scientists started on suitable countermeasures thus greatly reducing the ultimate tactical effectiveness of the enemy's new developments.

Now I must say a word or two about the protection of COMINT. First of all you have this very difficult psychological problem that our State Department officials are confronted with. This is best told in the late Secretary Hull's memoirs, and I will read you a little extract. He is talking about a meeting with Matsuoka with the Japanese Ambassador. "Actually I already knew the contents of the message. It contained a statement from Matsuoka to me that the German and Italian leaders were confident of victory that American participation in the European war would merely prolong it and bring about the destruction of civilization and that Japan could not injure the position of her Allies. We knew this because of the fact that our Navy and Army cipher experts, with remarkable ingenuity had broken the Japanese code and were deciphering government messages from Tokyo to Washington and other capitals, translating them and sending them to the State Department for our information. These intercepts bearing our codename MAGIC played little part in our early negotiations but were of great importance during thefinal phases. They enabled us to know many of the instructions the Japanese Foreign Minister was sending to Nomura and to other Japanese representatives. It gave us a check on what Nomura

was reporting to Tokyo concerning the conversations he was holding with me and they showed that the Japanese Government was going ahead with the plans even while talking peace with us. I looked upon them as I would look upon a witness who was testifying against his own side of the case. I naturally had to be careful, never to give Nomura the slightest impression of this special knowledge. I had to take care to keep our conversation limited to the knowledge I might have gained from him or from normal diplomatic sources. This is a trick. Try it yourself someday and see whether you can remember where you got a certain piece of information from. So as to safeguard the security of these messages, I named one of my secretaries to handle them, keep track of them and make sure that they were returned to the Navy or destroyed." He mentions the Navy, I will add that we had an agreement between the Services as to who would distribute to where. Up until we had such an agreement, it was a little like, well little boys running to the teacher with news, the Army trying to get to the President before the Navy, and so on. Well, this was no-go so an arrangement was worked out whereby Army would decrypt and translate messages bearing the even date, that is cryptographic date, and the Navy would handle messages bearing the odd date and this way we divided the traffic up more or less equally. The Army would distribute to the Chief of Staff and bla bla bla and the Navy would distribute to the President and bla bla bla so that there would be no competition in running to these places and getting there ahead of the other Services.

Now, a few words with regard to the organization required for effecitve COMINT operations. Intercept of foreign communications and subsequent processing