LECTURE V

HISTORY OF THE INVENTION AND DEVELOPMENT OF CIPHER DEVICES AND MACHINES.

Three or four years ago I was asked to give a lecture before the Communications-Electronics Division of the Air University, USAF, on the subject of communications security (COMSEC).

About that time there was be r 'ummered into our ears over the radio a slogan concerned with , obile traffic safety rules.

The slogan was: "Don't learn your traffic laws by accident!"

I thought the slogan useful as the title of my talk but I modified it a little: "Don't learn your COMSEC laws by accident'"

I began my talk by reading Webster's definition of the word accident.

I know, of course, that this group here today is not concerned particularly with COMSEC duties of any sort. But the definition of the word accident will nevertheless be of interest in connection with what will be said in a moment or two, so I'll read Webster's definition if you'll bear with me.

Webster: "Accident" - literally, a befalling.

a. An event that takes place without one's foresight or expectation, an undesigned, sudden, and unexpected event.

b Hence, often, an undesigned and unforeseen occurrence of an afflictive or unfortunate character, a mishap resulting in injury to a person or damage to a thing, a casualty, as to die by an accident

Having defined the word, I'll now proceed by relating an interesting, minor, but nevertheless quite important episode of the war in the Pacific Theatre during WWII, and I will introduce the account of that episode by saying that:

During the war, the President of the United States, Chief of Staff of the Army, the Commander-in-Chief of the U.S. Fleets, and certain other high officers of Government journeyed several times half-way around the world to attend special meetings and conferences They apparently could go with safety almost anywhere--they met with no "accident". On the other hand, the Japanese Commander-in-Chief of the Combined Fleet, Admiral Isoroku Yamamoto, went on an inspection trip in April 1943, the sequel to which may be summarized by an official Japanese Navy Department communique reading in part as follows: "The Commander in Chief of the Combined Fleet, Admiral Isoroku Yamamoto, died an heroic death in April of this year, in air combat with the enemy while directing operations from a forward position."

As is often the case, the communique didn't tell the whole truth: Yamamoto didn't die "in air combat with the enemy while directing operations" - he met with an "accident". I don't know who first used the following terse statement but it's decidedly applicable in this case: "accidents don't happen--they're brought about!" Our Navy communication intelligence people were reading the Japanese Navy's high command messages, they had Yamamoto's schedule to the day, hour and minute that Yamamoto would leave Truk, the time he would arrive at Buka and leave Buka for Kahilli or Ballale, they also knew what his escort would be and so on. It was relatively easy to bring about the "accident". Our top Commander-in-Chief journeyed with safety because the communications connected with his various trips were secure, the Japanese Commander-in-Chief journeyed in peril because his communications were insecure His death was no accident in the dictionary sense of that word, it was brought about.

The Yamamoto incident later gave rise to a somewhat amusing exchange of top secret telegrams between Tokyo and Washington, and after the war was all over these telegrams turned up in The Forrestal Diaries, Chapter III, pp. 86-87.

Extract from the "Forrestal Diaries," Chapter III, "Foretaste of the Cold War," pp. 86 and 87.

The formal surrender took place on the deck of the USS Missouri in Tokyo Bay on September 2. The mood of sudden relief from long and breaking tension is exemplified by an amusing exchange a few days later of "Urgent: Top Secret" telegrams which Forrestal put into his diary. In the enthusiasm of victory someone let out the story of how, in 1943, Admiral Isoroku Yamamoto, the Japanese naval commander-in-chief and architect of the Pearl Harbor attack, had been intercepted and shot down in flames as a result of the American ability to read the Japanese codes. It was the first public revelation of the work of the cryptanalytic divisions, and it brought an anguished cable from the intelligence unit already engaged at Yokohama in the interrogation of Japanese naval officers: "Yamamoto story in this morning's paper has placed our activities in very difficult position. Having meticulously concealed our special knowledge we have become ridiculous." They were even then questioning the Japanese officer who had been responsible for these codes, and he was hinting that in face of this disclosure he would have to commit suicide. The cable continued: "This officer is giving us valuable information on Japanese crypto systems and channels and we do not want him or any of our other promising prospects to commit suicide until after next week when we expect to have milked them dry . . ."

Washington answered with an "Operational Priority: Top Secret" dispatch"

"Your lineal position on the list of those who are embarrassed by the Yamamoto story is five thousand six hundred ninety two All of the people over whose dead bodies the story was going to be publishhed have been buried. All possible schemes to localize the damage have been considered but none appears workable. Suggest that only course for you is to deny knowledge of the story and say you do not understand how such a fantastic tale could have been invented. This might keep your friend happy until suicide time next week, which is about all that can be expected . ."

But not many years passed before the Japanese began to realize what had happened to them in the cryptologic battles of World War II. For example:

"Rear Admiral Tomekichi Nomura, the last CNC in the Japanese Navy, said:

' . . Not only have we been beaten in the decisive battles of this war but also we lost the communications war. We felt foolishly secure and failed to take adequate measures to protect our own communications on one hand while on the other we failed to succeed in breaking into the enemy's traffic. This is undoubtedly one of the major reasons for our losing battles, and in turn one of the major contributing factors to the loss of the war. We failed in communications."

". . Our Navy was being defeated in the battle of radio waves. Our cards were bad, and the enemy could read our hand. No wonder we could not win in this poker game!"

YOKOI, Toshiyuki - The Story of the Japanese Naval Black Chamber.

Books recently published in Japan by former Japanese military and naval officers come out quite openly with statements attributing their defeat to poor COMSEC on their part and excellent COMINT on our part.

Read from Midway book

Lest you infer that our side didn't meet with any COMSEC "accidents', let me say that we had plenty--but these were not attributable to serious weaknesses in our COMSEC devices, machines, and rules but to human failure to follow the rules implicitly, or--and this hurts in saying it--to weaknesses in the COMSEC devices, machines and rules of some of our allies.

Take, for instance, the heavy losses the U.S. Army Air Corps sustained in their air strikes on the Ploesti oil fields in southeastern Europe. We lost several hundred big bombers because of weaknesses we didn't realize existed in Russian communications. Those big raids constituted field days for the German fighter commands--because merely by T/A work, and simple at that, they knew exactly when and where our bombers were headed' When we found out, it was too late!

This incident leads me to say that the COMSEC weaknesses of our allies and friends even today leads to a rather serious illness which afflicts our high-level authorities from time to time. I've given the disease a name: Cryptologic schizophrenia.

It develops when one is torn between an overweening desire to continue to read friendly traffic by cryptanalytic operations when one knows that that traffic should be made secure against one's enemies!

Thus far, no real psychiatric or psychoanalytic cure has been found for the illness. The powers that be have decreed that the illness will be avoided by the simple ruling that COMSEC interests will always over-ride suppressed COMINT wishes.

You will understand that this problem is a rather serious one in connection with our relations with certain of our allies in NATO. I may add that U.S. and U.K. physicians collaborate very closely in treating their own patients for the cryptologic schizophrenia and in applying remedies where possible in bolstering COMSEC weaknesses in NATO.

Today we are going to see some slides which will mark and illustrate important milestones in the history of the invention and development of cipher devices, cipher machines, cipher apparatus, and, if there is time, rules for establishing and maintaining COMSEC.

The need for these things arose as a consequence of the constantly increasing necessity for more security in military and diplomatic communications, more especially after the advent of telegraph, cable, and radio communications subsequent to the discoveries of the pioneers in the field of electrical invention and development.

It soon became obvious that the so-called "pencil and paper" cipher systems--and a little later, the so-called "hand-operated" cipher devices--had to give way to machines and mechanical, mechanico-electrical, and now, to electronic machines As mechanization and automation progresses in our civilization, similar progress has to follow in communications, especially in military, naval, air and diplomatic communications

45
The earliest picture of a cipher disk, from Alberti Trattati in cifra, Rome, c. 1470 "Oldest tract on cryptography the world now possesses."

45.2
The Myer disk, patented 14 Nov 1865.

45 4
The Alberti Disk reincarnated in the U S. Army Cipher Disk of 1914-18

Somebody once said that the very nice looking document with seal and red ribbon that is issued when the U.S Patent Office grants a patent is nothing but a fine looking invitation to participate in a lawsuit for infringement. But the person being hurt by infringement upon his patent must be alive to file the suit--or at least his heirs and/or assignees should be alive I doubt however that Alberti or his heirs and/or assignees were alive to contest this patent, issued in 1924, for a cipher disk practically identical with Alberti's disk of 1470!

47 The cipher disk finally patented in 1924 -- Huntington Patent. Shows that the Patent Office does not have general information on cryptography because of the secrecy involved.

47 1 Cipher disk used by Nazis in 1936.

48 Original Wheatstone cipher device (invented and described in 1879). First important improvement on the Alberti disk

49 The modified Wheatstone cipher device Produced by the British Army 1917-18 but never used because of solution by Wm F. Friedman -- story of solution.

49.1 The Decius Wadsworth ciphher device (invented and built in 1817 when Colonel Decius Wadsworth was Chief of Ordnance).

49.4
The Bazeries cryptographe cylindrique (1901) as shown in his book "Les chiffres secrets devoiles". But he may have described this in his article "Cryptograph a 20 rondelles-alphabets" Comptes rendus, Marselles, 1891.

49.5
Bazeries, Etienne.

50
First page of Jefferson's description of "The Wheel Cipher"

50.1
Second page of Jefferson's description showing his calculation of the number of permutations afforded.

160.1
Original model of Hitt's strip cipher (The Star Cipher).

50 4
Parker Hitt's model of strip cipher (1916) Story of solution at Riverbank Laboratories of test messages prepared by Mrs. Hitt.

159.1
The first six messages and their plain texts of Mauborgne's set of 25 challenge messages.

50.2
U.S. Army Cipher Device M-94.

50.5
Early attempts to use cylindrical cipher device principle but with variable alphabets (M-136)

50 6 (M-137)

50.7 (M-138-T1)

50.8 (M-138)

50 11 (Folding M-138)

50.12
U S. Army cipher device, Type M-138-A (with Russian legends). Story of Russian legends and how they came to be there.

51
European model of strip cipher

52
European model disassembled Syko strip cipher. Court awards ~~£~~35,000 to "inventor".

54
The Kryha cipher machine.

55
A German mathematical dissertation on the Kryha

Merely number of permutations and combinations a given machine affords like -- has nothing to do with the case or at least not much. Depends on nature of permutations and combinations, what they are cryptographically. For instance, the principle of monoalphabetic substitution as in Gold Bug - 26! cipher alphabets or the large number:- 403,291,461,126,605,635,584,000,000
quad/trillions/billions/millions

(Four hundred and three quadrillions, two hundred ninety-one thousand, four hundred and sixty-one trillions,
One hundred twenty-six thousand, six hundred and five billions,
Six hundred thirty-five thousand five hundred and eighty-four millions--
"and a frew".

Estimated would take 1000 million men working a thousand million years to do the major part of writing these alphabets out -- scroll would reach from earth beyond the planet Mercury'

All the preceding examples of cryptographic aids are in the category of what may be termed "pencil and paper" or "hand-operated" aids. These, of course, had to give way to more rapid and more secure means for crypto-communications, and this meant machines of one sort or another. There was pressing need in the military and naval services for two machines:

1. A small machine for low echelon or field use.

2. A larger machine for rear echelon and high-command use.

Let's take up the first of these two types.

171.1
171
M-161 Signal Corps model made at Fort Monmouth (Efforts to develop field machine and tell story re obtuse director of S.C. Labs. Note power source.

164
Boris C. W. Hagelin Does a "hysteron-proteron" in inventing C-36.

7Ø.1
Converter M-2Ø9.

7Ø 3
Example of American resourcefulness and skill under difficulties Two GI's in Italy mechanize the M-2Ø9. (The cartoon, showing a couple of GI's with a home made still, and the legend: "Yes, but will it work?")

26Ø.1
Hagelin CX-52. Double tape-printing. Key wheels removable. Irregular stepping. Non-guaranteed cycle

260
Hagelin CX-52 (and its fundamental weakness)

The big problem in the use of devices and machines which are of the key-generator or additive (or subtractor) type is the fact that when the alphabets involved are known alphabets, solution of a depth of two is generally possible.

261-A
Example of solution of polyalphabetic encipherment with book key and known alphabets, in this case reversed standard.

261-B
Continuation.

262
Hagelin (M-209) Solution: "A depth of two"

We come then to the so-called rotor machines, which are not based upon key-generator principles but are permutation machines. We come now therefore to the history of rotor machines.

58.1
The Swedish electrical machine B-21. (Original Aktiebolaget Cryptographe B-21. Mention Boris C. W. Hagelin.)

59
Swedish machine connected to electric typewriter.

65
The keyboard electrically-operated B-211 Swedish machine (Self-contained, instead of separate typewriter.)

The original (commercial) Enigma cipher machine. (Later used with one improvement by Germans in World War II.)

71
Come now to American developments. Edward H. Hebern. How he became interested in cryptography and invented a cipher machine.

172
The first Hebern machine. (Manufactured for use by the Ku Klux Klan.)

71 1
The first Hebern printing model. Still a one-rotor machine! Where did he get the idea of cascading rotors?

71.2
71.3
Hebern rotors -- variable wiring possibilities! 13 to one side and 13 to other.

172.1
3-rotor Hebern

72
165
The 5-rotor Hebern machine. (Story of solution)

172.2
First Hebern machine built in accordance with Navy specifications.

172.x
Hebern model S.I.S. Solved on challenge by Navy.

172.10
One of Hebern's developments for the Navy, after his release. Solenoid operated design built according to Navy specifications. (This is the one that

wouldn't work--but Hebern said the contract didn't specifically state that it had to work. He insisted on being paid--and was' It was the last job he did for the Navy. (One Navy file insisted that Navy had an Admiral in Navy District HQ in San Francisco just to keep Hebern out of jail so he could finish the Navy contract!)

Navy has enough of Hebern and goes in for its own development.

Fifteen years later Hebern Co. and heirs institute suit in U.S. Court of Claims for $50,000,000! Probable settlement by now for few thousand dollars.

Collaboration and cooperation between the Army and Navy on cryptographic research and development notable for its absence in those days. Each service had its secrets!

170A
U.S. Army Converter M-134-T1. Basic principle -- external keying element.

170 2
Converter M-134. Rear view.

170.7
Converter M-134 - with printing!

170.9
U.S. Army Converter M-134-A.

172.4
Original Navy Mark I ECM with Boudin wires! Only 15 starting points!

172.5
First production model of Navy Mark I

173
Army and Navy finally collaborate! SIGABA-ECM.

174
SIGIVI or Basket.

SIGABA-ECM withheld from British. Battle to give to British. Finally given in 1953. But during WWII had to intercommunicate. Therefore--the CCM.

74
74.1
74 2
The German Armed Forces cipher machine of WWII. Effects of solution. German lack of imagination! High speed machinery could do it but they lacked the imagination'

Say few words about American developments Hebern.

58
German 8-wheel printing Enigma. Captured in 1945 at Mittelfels. A failure!

German Naval Enigma -- differences between it and Army and Air Force enigma.

With growth of teletype communications the need for an practicability of automatic encipherment became obvious. The first attempt--the machine developed by the AT&T Co. (1918) in collaboration with the Signal Corps.

56
The AT&T Co. printing telegraph cipher machine (1918) (The original SIGTOT)
Story of solution

258
Problems of manufacture of tape. Our electronic tape production machines solve problem

60
The IT&T Co. teletype cipher attachment.

With the growth of teletype communications, cipher teletypewriter attachments were invented.

178
SIGCUM

179
SIGCUM - cover removed.

180
SIGCUM with B-131 set and teletype machine. SIGHUAD - a form of SIGCUM with one-time key features. Dangers of electrical radiation Dangers of depth

182
SIGNIN Wartime development. Lots of 'bugs'.

183
SIGMEW - CIFAX.

185
Ciphony. SIGJIP - Bell Telephone 1st development.

186
186 1
Ciphony and cifax machines. SIGSALY. Vocoder types.

New developments in cipher machines. AFSAM-7, AFSAM-9, AFSAM-15, AFSAM-36 and AFSAM-D21. "Integrated" equipments. Ciphony and its problems. SIGSALY.

Recognition and identification. Callsign. Telemetering. Television.

The professional cryptologist is always amused by the almost invariable reference by the layman to the "German code" or the "Japanese Code" or "the U.S code". To give an idea as to the miltiplicity of systems -- show next two slides.

236
Number of cryptographic systems in effect 7 December 1941 - October 1945. U.S Army and Army Air Forces only.

237
Number of holders of cryptographic materials. December 1941 - October 1945. U.S. Army and Army Air Forces only.

129
13Ø
Keeping track of crypto-material and accounting. Japanese incident of certifying to destruction by burning.

I will bring this talk to a close now by repeating the importance of the slogan we try to inculcate: "Don't learn your COMSEC laws by accident!"