COMMUNICATIONS INTELLIGENCE

Outline of Presentation by Mr. William F. Friedman, Consultant, Armed Forces Security Agency, at the Second Annual Communications Security Officers' Conference to be held at Brooks Air Force Base, 3-7 March 1952.

I. Introduction

A. Appreciation of opportunity to address the Conference

1. Impression that last year's conference, the first of its kind in the history of communication security in the Armed Forces of the U. S., showed considerable initiative, forward-looking viewpoints, and excellent understanding of the COMSEC field.

2. Above impression stengthened by excellent tone of this year's conference.

3. Much benefit to be obtained from the mutual exchange of ideas.

B. Particular appreciation of opportunity to address this Conference on communications intelligence

1. Relationship of communications security (COMSEC) and communications intelligence (COMINT) - close

ILLUSTRATION: During second World War the President, and other high-ranking U. S. Government officials journeyed at great distances without "accident." On the other hand, the plane carrying Japanese Commander-in-Chief, Yamamoto, on an inspection trip in April 1943 was shot down by U. S. planes. Yamamoto's death was no "accident." U. S. Navy communications were reading Japanese messages and knew the schedule, escort, etc., for the Japanese Commander-in-Chief. Our officials travelled in safety because our communications were secure; the Japanese Commander-in-Chief journeyed in peril because his communications were insecure. They were vulnerable to our COMINT.

C. Importance of COMINT

1. Has not always been appreciated

ILLUSTRATION: Story of Semiramis, the Persian queen, who had inscribed upon her tomb a message that if the cryptogram engraved thereon could be solved it would lead to riches beyond all dreams of avarice. Many hundred years later the message was solved

by an earnest student, only to find within the tomb a message in plain text that had he learned something more useful than the art of deciphering, he would not be in need of money.

2. In World War II was recognized as a vital military weapon.

ILLUSTRATION: Paragraph from Time Magazine of December 17, 1945 revealing the use of a cryptanalytic machine in World War II which deciphered Japanese diplomatic messages.

II. Communication Intelligence: History and Development

A. General remarks

1. Definition: all intelligence derived from the study of radio transmissions and other communications.

2. Objectives

a. To provide authentic information for policy makers, and appraise them of realities of the international situation, of the war making capacilities and vulnerabilities of foreign countries, and of the intentions of those countries with respect to war.

b. To eliminate the element of surprise from an act of aggression by another country.

c. To provide unique information essential to the successful prosecution, and vital to the shortening, of the period of hostilities.

3. General development

Communications intelligence, which is based on the science of cryptanalysis, has a long history inextricably bound up with the history of cryptography, which is the basis of communications security.

4. Limitations of discussion

a. Information on history and development of foreign countries is sparse.

b. Security considerations preclude;

(1) Comparison of foreign and U. S. systems or successes
(2) Discussion of current U. S. developments.

c. Personal experience limits discussion mainly to Army's cryptodevelopments.

B. History of Cryptology, Illustrated

1. Biblical examples

a. Jeremiah 25:26 and 51:41: Sheshakh a cipher for Babylon. (1)

b. Daniel 5:25-29: interpretation of MENE, MENE, TEKEL, UPHARSIN.

2. Examples from classical antiquity

a. Scytale used by the Lacedaemonians to send messages to field commanders. (2)

b. Simple substitution used by Julius Caesar.

c. Shorthand used by Tiro, the amanuensis of Cicero.

3. Ciphers of the 15th, 16th and 17th centuries.

a. Beginnings of modern cryptography found in Venice and the Papal States - 1400. (4.10)

Knowledge of basic weakness of monoalphabetic substitutions recognized and corrected by having high-frequency letters represented by more than a single character.

b. Earliest tract on cryptography and cryptanalysis written in 1474 by the Neopolitan, Simion Simonetta.

c. First extensive treatise on cryptography written by the German abbot, Trithemius, in 1531.

(1) Books burned as having been written in league with the Devil.
(2) Oath of secrecy still pertinent. (151)

d. Ciphers used in diplomacy

(1) Cipher alphabet used by Mary, Queen of Scots, circa 1545. (3.5
(2) Tables of the Italian cryptographer, Porta. (3.5 & 6.1)

(a) Greatest of early cryptographers
(b) Inventor of the camera obscura
(c) One of earliest cryptanalysts to solve a system of keyed substitution.

(3) Porta's Table - found among state papers of Queen Elizabeth, used to communicate with the English Ambassador in Spain. (6.1)

(4) Vigenere Square - not invented by Vigenere but reproduced by him. (5.1)

(5) Francois Vieta, founder of modern algebra. In 1589 as Privy Counselor Vieta solved the Spanish cipher system used by Phillip II of Spain, thereby being accused of sorcery. (5.2)

(6) Sliding-card cipher. Facsimile of one used later in reign of Queen Elizabeth. (3.7)

(7) "Two-word or two-alphabet" square cipher involving coordinates. (3.8)

Used in time of Charles I (1627) to communicate with ambassadors in France and Flanders.

4. Ciphers of the American Revolution

a. Ciphers used by the British and the Americans were almost identical, many of the British messages being solved by an American, a "cipher expert to Congress."

b. Examples of use of cipher

(1) Jeffersonian syllabary, constructed on the two-part principle. (6.2)

(2) Ciphers used by Benedict Arnold in communication with British. (6.8)

5. Marked advances - 19th century

a. Solution of Egyptian hieroglyphics by a Frenchman, Jean Francois Champollion, about 1821 represents greatest linguistic achievement of 19th century. (4.0)

(1) Solution based on tri-lingual inscription on Rosetta Stone. (4.1)

(2) Examples of cartouches from the Stone. (4.2)

(3) Certain writings of the Egyptians cryptographic in character. (4.6)

b. Literary interest in cryptography exemplified by tales of Edgar Allan Poe; 1842 the Gold Bug.

c. Civil War

(1) Confederate cipher device based on principles of the Vigenere square. (7)

(2) Examples of route cipher used by Federal Army.

(a) Message from Lincoln to Burnside. (8)
(b) Message to General Grant. (10)

d. Franco-Prussian War
Example of micro-photography used by French in seige of Paris. (128)

6. Decline in cryptography 1864-1917

a. Military codes based on commercial codes.

Slater's code of 1906, "Telegraphic Code to Insure Secrecy in the Transmission of Telegrams" based almost word for word on "Telegraphic Code to Insure Secrecy in the Transmission of Telegrams," by J. F. Gregory published in 1885. (214)

b. Chief Signal Officer personally prepared suitable code in 1899.

c. "Cipher of the War Department"

First published in 1902 by the Adjutant General; revised in 1906.

d. War Department Telegraph Code

(1) Printed in 1915 by a commercial firm in Cleveland. (216)

(2) Only code when U. S. entered war in 1917.

(3) Informed by British that the code was not safe to use.

7. World War I

a. New era of communications and cryptology

(1) Hertz's discovery of so-called Hertzian waves.

(2) Marconi's demonstration of signalling by wireless.

b. Tactical systems used by belligerents.

(1) Cipher system used by Russians based on Vigenere square. (11)

(2) Front-line system used by French a transposition system with columnar key. (12)

(3) System used by Italian army also a variation of Vigenere square. (13)

(4) System used by Germans: the ADFGVX cipher. (14)

Early AEF examples of traffic analysis and traffic intelligence based on intercept and solution of ADFGVX systems. (15, 14.1)

(5) Playfair system used by British and Americans.

(a) Invented not by Lord Playfair but by Sir Charles Wheatstone. (23)
(b) Description of encipherment.
(c) Early description of solution published in 1914 by J. O. Mauborgne, later Major General and Chief Signal Officer. (159)

(6) Proposed cipher device of British Army.

c. Codes and code systems of World War I.

(1) Prior to World War I were thought impractical for tactical use.

Limited to commercial or diplomatic usage.

(2) Germans first used field codes in 1916; soon followed by Allies. (20)

(a) Early AEF codes like the "Baseball Code" of the 52d Infantry Brigade inadequate. (21)
(b) Field codes of Allies later very good. (19, 22)

d. Famous cryptograms of World War I.

(1) Zimmermann message which brought the U. S. in on the side of England. (28, 29)

(2) Waberski telegram. (25, 25.1)

(3) Sabotage messages connected with the Kingland fire and the Black Tom explosion. (127)

(4) Messages pertaining to the Hindu revolt incited by the Germans, (33)

(a) Messages solved by Friedman
(b) Dramatic ending in court scene

e. Cryptograms from peace time.

(1) Oil scandal in President Harding's regime. (38)

(2) Rum-runners of Prohibition days. (37)

(3) Solution of messages for Secret Service. (44.1)

8. Cipher Devices

a. Invention and introduction into wide usage of radio brought advances in cryptographic methods, particularly the invention of cryptographic devices and machines.

b. Brief review of history of cipher devices.

(1) Disc from book by Alberti, 1470 (45)

(a) Patented in 1865 by Major Albert J. Myer then Chief Signal Officer (45.2)

(b) Used by U. S. Signal Corps from 1910 to 1918. (45.4)

(c) Patented again in 1924.

(2) Cipher device developed by British in World War I and distributed on Western Front. (47)

(a) Modeled on the Wheatstone cipher device (invented in 1870). (48)

(b) Solved by Friedman at Riverbank Laboratories before it was actually in use. (157-Fabyan)

(c) Comparison with Decius Wadsworth cipher device invented in 1917. (49.1)

(3) Bazeries' "cipher cylinder" (49.5, 49.4)

Comparison with the device invented by Thomas Jefferson. (50)

(4) Same system invented independently in form of strips by Colonel Parker Hitt, U. S. Army. (160.1, 160)

Solved by Friedman at Riverbank Laboratories.

(5) Cylindric principle adopted by U. S. Army Signal Corps in 1918 as the M-94. (50.2)

(6) Adaptation of sliding strip form by U. S. Army as Cipher Device M-138. (50.8)

(7) AT&T Company Machine

(a) Produced in 1918 as the first one-time tape cryptographic transmission machine. (56)

(b) Solved by Friedman at Riverbank Laboratories.

(8) Hebern Cryptographic machines (71)

(a) Early machine with one wheel (71.1)

(b) Five-wheel machine produced in collaboration with Navy. (72)

1. Machine solved by Friedman before final contract was drawn. (165)
2. Hebern reduced to penury.

(9) Foreign Cryptodevelopments

(a) Commercial Enigma built in Europe in early 20's and sold on commercial market until 1933 when it was adapted for German military use. (57) (74.2)

(b) Kryha, German machine built for commercial use and considered unsolvable, but in reality solved with ease. (54) (55)

(c) Swedish machine B-21 of same period. (58.1)

(d) Joined to a Remington electric typewriter, this becomes a printing cipher machine. (59)

(e) Later modified to have the printing mechanism self-contained in the cryptograph - the Swedish 211. (65)

(10) Types of teletype cipher attachments.

(a) AT&T Company machine mentioned above in 8(8).

(b) IT&T Company machine invented by Colonel Hitt after his retirement from the Army in 1925. (60, 64)

(c) Automatic Electric Company of Chicago failed.

(d) IBM Company failed.

(e) Successful crypto-attachment for teletype finally developed by U. S. Army in 1943.

(11) U. S. Army Cryptomachines

(a) M-209 based on Swedish invention in (10)(c) above, mechanized in field. (70.1, 70.2) (70.3)

(b) Converter M-161 (171)

(c) Converter M-134A (170.8)

(d) Converter M-134C (SIGABA/ECM) (173)

9. Cryptanalytic aids

a. History of development

(1) First cryptanalytic aid developed by Friedman at Riverbank Laboratories in 1916. (131)

(2) Use of IBM machinery after 1934. (134, 135)

(3) Use of high-speed machinery.

(4) Recent development of electronics cryptanalytic gadgetry.

b. Advantage of machines is that they perform at a high rate of speed, accurately and without need for rest, relaxation etc., the processes which the human brain can perform at a much slower rate.

c. Examples

(1) Analogs for decipherment (139, 145, 144)

(2) IBM Standard Tabulator for use in locating repetitions. (141)

(3) Slide run unit for comparing messages. (138)

(4) The "Camel" and the Camel Code Indicator. (140,146)

(5) The "Auto-scritcher" or "Rodin". (143)

III. Conclusions

A. Manner of employment of communications intelligence.

1. Use in war to shorten hostilities.

a. Revealed by Pearl Harbor investigations.

b. Noted in letter of General Marshall to Governor Dewey,

(1) Hitler's intents in Europe known from messages of Japanese Ambassador in Berlin to his Government.

(2) Battle of Coral Sea and Midway based on deciphered messages which made concentration of our naval forces possible.

(3) Operations in Pacific guided by deciphered messages.

(4) Heavy losses to enemy convoys from submarine action.

B. Successful COMINT requires large organization.

1. World-wide intercept.

2. Expeditious forwarding to processing center.

3. Central processing organization for concentration of highly skilled personnel and specialized machinery.

4. Evaluation, integration, collation.

5. Transmission of intelligence to operational commanders.

C. COMINT activities must be co-ordinated with tactical operations

1. Field commanders must give adequate cover to operations based on information obtained from COMINT.

a. Minor tactical success may result in loss of valuable intelligence from an enemy crypto system which has an area - or world-wide distribution, since the enemy may guess the source of information.

b. Destruction of enemy communication system or element thereof may result in loss of valuable COMINT.

2. Conversely producers of COMINT must be fully oriented on the current tactical situation.

a. In order to give optimum coverage and to know where to place maximum effort.

b. In order to give proper evaluation to the results.