~~SECRET~~

JOINT AMERICAN MILITARY ADVISORY GROUP, EUROPE
20 GROSVENOR SQUARE
LONDON, W. 1.

COPY

FC 311.5 9 Feb 1951

SUBJECT: Hagelin Machine Converter (Cipher), M-209-B File under NATO

TO: Armed Forces Security Agency
The Pentagon
Washington 25, D. C.

1. In consideration of the NATO code and cipher problem, the European NATO Tri-Regional Cipher Committee has provisionally set up the following categories of ciphers:

a. Top Level Ciphers. To provide for the needs of high military and diplomatic authorities. This part of the problem is supposedly now solved by the provision of the British Typex Mark II Machine.

b. Second Level Ciphers (strategic). To provide for the needs of units down to and including Air Force Groups, Army Divisions and major naval vessels.

c. Third Level Ciphers (tactical). To provide for the needs of smaller headquarters and units.

2. On 30 January 1950 the Western European Region (NATO) Cipher Committee met in Paris to consider a [redacted] for NATO adoption and joint use as a second-level cipher. This machine proved to be nothing more than a U. S. built, Army Signal Corps, Machine Converter, M-209-B.

3. The [redacted] representative admitted that the M-209-B had virtually no security, but stated that if the machine were equipped with the [redacted] modification described in enclosure 1 encrypted traffic would be "absolutely secure."

4. The [redacted] representative explained that the proposed [redacted] modification to the M-209-B was protected by [redacted] patents and that it would therefore have to be manufactured by [redacted] firms or by foreign firms under contract. He also stated that since the model being exhibited was only a prototype it would probably take about one year before all NATO units could be equipped with the modified M-209-B.

~~SECRET~~

~~SECRET~~

COPY

5. Representatives were requested to be prepared to state at the next meeting:

a. Whether their nations were prepared to accept, on a joint Army-Navy-Air Force basis, the M-209-B with the [redacted] modification as a second-level cipher machine.

b. Whether their nations were prepared to accept, on a joint Army-Navy-Air Force basis, the M-209-B in its unmodified form as a third-level cipher machine.

c. Their nations' short and long term numerical requirements for the machine (if accepted) bearing in mind that priority should be given to international traffic.

6. If, as is the opinion of personnel of this headquarters who have operating crypto experience, the U. S. position in regard to the [redacted] proposal will probably be one of non-acceptance, is any U. S. counterproposal available? This counterproposal might take the form of a definite U. S. commitment to release a comparatively secure system, such as a strip cipher with the strip eliminator table, or it might take the form of a firm Standing Group statement to the effect that the matter was under active consideration and that a solution was expected at some definite date in the near future. The opinion of this headquarters is that the [redacted] proposal is a retrograde step and should be overruled. This, however, may be difficult, since the M-209-B with the [redacted] modification is the only low-level cipher device now available to NATO, and the European nations may be inclined to adopt it for lack of something better.

7. U. S. information and guidance pertaining to the contents of paragraphs 5 and 6 above is required by the U. S. representative on the Cipher Committee prior to the next meeting on 27 February 1951.

/s/
A. FRANKLIN KIBLER
Major General, USA
Director

CC: JCEC
CNO(DNC)
G-2 (ASA)
Dir. Communications (USAF)

Enc. 1: [redacted] Modification to M-209-B

~~SECRET~~

SECRET

COPY [redacted] MODIFICATIONS TO HAGELIN MACHINE CONVERTER, M-209-B

1. The [redacted] modification to the M-209-B converter consists of a new Indicating Disk-Type Wheel assembly which is interchangeable with the corresponding assembly supplied with the standard M-209-B. The standard component may be removed by unscrewing the thumbscrew in the center of the Setting Knob shaft and the modified French assembly inserted.

2. The differences between the standard Indicating Disk-Type Wheel assembly and the [redacted] assembly are threefold:

a. On the standard assembly the Type Wheel consists of a straight alphabet arranged in reverse order. On the [redacted] modification the alphabet on the Type Wheel is capable of being scrambled according to a pre-arranged sequence because the individual letters of the alphabet are quickly removable and interchangeable.

b. On the standard assembly the Indicating Disk consists of a straight alphabet arranged in normal order. On the [redacted] modification the alphabet on the Indicating Disk is capable of being scrambled according to a pre-arranged sequence because the individual letters of the alphabet are quickly removable and interchangeable.

c. On the [redacted] modification there is an additional disk mounted to the left of, and adjacent to, the Indicating Disk, on which is printed a series of unmovable consecutive numbers; two series of zero through nine and one series of zero through four; the space on the numbered disk opposite the letter "Z" on the Indicating Disk being left blank. This is intended to permit direct encryption of numbers without spelling them out as words, each number being represented by a letter, but with the possibility of the individual numbers zero through four being represented by three different letters and the remaining numbers by two letters.

3. One feature which may be cryptographically undesirable is the fact that the letters "Z" on both the Indicating Disk and the Type Wheel are always fixed in the same position relative to each other in order to form a common base for the scrambled Type Wheel and Indicating Disk alphabets employed.

Inclosure 1

SECRET