FSC53/EX/R(2)
010

12 June 1953

REPORT OF THE

US-UK CONFERENCE ON THE COMMUNICATIONS SECURITY OF [redacted]
NATO COUNTRIES
HELD IN WASHINGTON, 5-12 JUNE, 1953

THE PROBLEM

1. To consider the insecurity of NATO communications and of the national communications of NATO countries, including a review of the conclusions of the 1951 US/UK Conference on the Security of [redacted] Communications, in order:

a. To determine whether the NATO Governments should be approached with a view to improving their communications security;

[redacted]

c. To develop, if such an approach should be made, (1) a specific plan for improving the security of NATO communications and of the national communications of NATO countries and (2) a specific plan for approaching the NATO Governments.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

I. ASSUMPTIONS AS TO THE COMINT CAPABILITY OF THE USSR

2. This Report is predicated upon the assumption that:

a. The capabilities of the USSR to intercept and exploit radio communications are at least equivalent to those of the US [redacted]

b. The USSR monitors all landline communications passing through its own or satellite territory. The possibility that it has access to other communications passed solely by landline cannot be excluded, but there is no evidence to assess the extent of this possibility. Any traffic obtained by the USSR from landlines can be exploited to the same extent as traffic obtained from radio transmissions.

II VALUE TO THE USSR OF COMINT DERIVED FROM THE COMMUNICATIONS OF NATO COUNTRIES (see Footnote 1)

3. [redacted] communications ciphers in peace time.

a. Although the US and UK views differ as to the current value

[redacted]

Footnote 1.

It should be noted that the security system of NATO provides sufficient protection for "COSMIC" and "NATO" communications passed electrically. However the NATO security system does not provide protection for national communications carrying related information, nor do all the NATO countries confine "NATO" and "COSMIC" communications to approved channels. Recent

[redacted]

the NATO procedures.

Footnote 2.

[redacted]

Footnote 2 (Continued)

[redacted]

b. The value to the Russians of the COMINT derived from the communications of individual NATO countries will vary directly with both (1) their vulnerability and (2) the extent to which they contain information, the compromise of which would be damaging to the US or the UK.

(1) [redacted] are on this basis alone thought to represent no current or predictable source of valuable intelligence to the USSR.

(2) [redacted] volume of their communications and the relatively slight participation of these countries in matters which would involve critical information, are also thought to represent no current or predictable source of valuable intelligence to the USSR.

(3) [redacted]

(4) [redacted]

(5) [redacted]

of valuable intelligence to the USSR.

4. Diplomatic ~~ciphers~~ communications in wartime.

It is considered that on outbreak of active hostilities the value to the USSR of the information derived from the communications of NATO countries would be greatly increased.

5. Armed Forces ~~ciphers~~ communications in peace and war.

[redacted]

are [redacted] that ought to be denied to the Communists.

b. In general it is thought that under peace time conditions Armed Forces communications are unlikely to be an important source of valuable intelligence to the USSR. In cases of limited hostilities, [redacted] it is, however, considered that vulnerable Armed Forces ~~ciphers~~ communications are a menace to the national interests of the UK and the US and in the case of general hostilities would become a real danger.

III. VALUE TO THE USSR OF INTELLIGENCE ON NATO COUNTRIES DERIVED FROM NON-COMINT SOURCES

6. Clandestine Sources

a. Non-COMINT clandestine means of obtaining intelligence cannot be regarded as a complete substitute for COMINT as a source of intelligence. In particular, in areas where COMINT is effective, clandestine intelligence is generally less timely, less complete and less authoritative than COMINT. Information from clandestine sources needs a sometimes difficult process of evaluation before it can be accepted; is dependent on the availability of communications; and is frequently subject to considerable delay before it is received [redacted] value of intelligence from clandestine sources can frequently be greatly increased by correlation with COMINT. Moreover, the capacity to sustain successful clandestine arrangements to obtain intelligence often depends upon information derived from COMINT.

b. Although it must be presumed that penetration of NATO nations by agents of the USSR exists and will continue to exist, it is considered that, at least, so far as the US, UK, [redacted] are concerned, this is becoming increasingly difficult.

(1) [redacted] there has been a definite improvement in the overall security situation, and further improvements are planned. In the Armed Forces and security agencies specific steps have been taken to place in effect a security system which is [redacted] of December, 1952, ~~However,~~ and there remain significant handicaps--political and administrative--to improvement. The level of overall security in [redacted] In the light of these developments it cannot be assumed that clandestine sources of intelligence for the USSR will be significantly reduced in [redacted] in the near future. Nevertheless, the operation of clandestine sources is expected to become increasingly difficult, and, therefore, it is felt that the USSR could not find adequate compensation for the loss of potential COMINT through increased clandestine activity.

(2) As regards other NATO countries from which the potential value of COMINT is estimated to be high there is insufficient collated evidence available to this conference to assess the state of their security. In particular there is

EO 3.3(h)(2)
PL 86-36/50 USC 3605

not available any report such as that produced by

[redacted]

c. In time of war, due to the introduction of security measures which are not possible in peacetime, clandestine operations become much more difficult. The ready means of communication afforded by diplomatic missions and consulates are also no longer available. It is therefore considered that the value of information from clandestine sources will be substantially diminished at least initially by an outbreak of hostilities.

7. Other Sources

a. It is difficult to assess to what extent open sources (newspapers, trade publications, public documents and statements, etc.) or diplomatic reportage could be a

[redacted]

sources and that, even during peacetime, this intelligence may increase substantially in volume and value at any time. In wartime, censorship and other extraordinary security measures, will reduce drastically the flow of intelligence from such sources, and the value to the USSR of any available COMINT will be correspondingly increased.

b. It should be noted that, as in the case of clandestine sources, the value of intelligence from other sources can be greatly increased by information derived from COMINT.

[redacted]

V SECURITY AND INTELLIGENCE FACTORS AFFECTING ACTION TO BE TAKEN

10. The nature of any action taken to reduce the potential damage to the national security of the US and UK created by the vulnerability of the communications of NATO countries will be determined largely by technical considerations. From the point of view of intelligence and general security consideration, however, such action must:

a. be designed to rectify effectively inadequate communication security practices of NATO countries throughout.

[redacted]

c. [redacted]

d. [redacted]

VI TECHNICAL FACTORS AFFECTING ACTION TO BE TAKEN

11. Inasmuch as it appears to be impractical to attempt corrective action by provision of new equipment, action should initially be aimed at the improvement of available cryptosystems and communications practices wherever possible. It is considered that such improvement can be effective.

12. No matter what initial approach is agreed the proper authorities for handling issues of this nature are the communications security agencies of the NATO nations concerned. This consideration is re-inforced by that stated in paragraph 11 above. It is therefore important to associate the communications security agencies with the action proposed at as early a stage as possible. The same reasoning applies to the use of communication security authorities to originate the action. Further factors in support of these considerations are that:

a. The security and intelligence factors enumerated in paragraph 10 above make this the safest procedure.

b. For reasons of economy it is desirable that existing agencies

c. [redacted]

communications security channels. Two examples of such instances are enclosed herewith as Appendix A.

13. The interrelationships between transmission security and crypto-security are such that a completely successful program to improve communications security must deal effectively with both.

14. It is considered that there is no way to deal effectively with disregard of "COSMIC" and "NATO" communications security regulations

[redacted]

tions security attitude and practices of the offending countries.

VII OUTLINE OF PROPOSED ~~GENERAL CONSIDERATIONS AFFECTING ACTION TO BE TAKEN~~

15. The Conference is agreed that the factors enumerated in paragraphs 10 through 14 above can best be met by using the existing communications security machinery of the Standing Group. It is realized that the Standing Group cannot issue directives about matters outside the scope of the military aspects of NATO, but it would seem right to use existing Standing Group machinery in an advisory capacity, since the security of NATO is jeopardized by insecure national communications.

[redacted]

means to be determined and agreed by appropriate US and UK authorities, with a view:

[redacted]

Group as the NATO mechanism to improve the communications security of the other NATO nations and after successful initiation of the discussions described in 18b above, the Standing Group will issue a memorandum to all member nations which will:

a. Express disquiet at the potential danger to overall NATO security of the insecurity of the national communications, either diplomatic or military, of any NATO nation, pointing out that the present of NATO as a whole depends upon the security of each individual [illegible] nation.

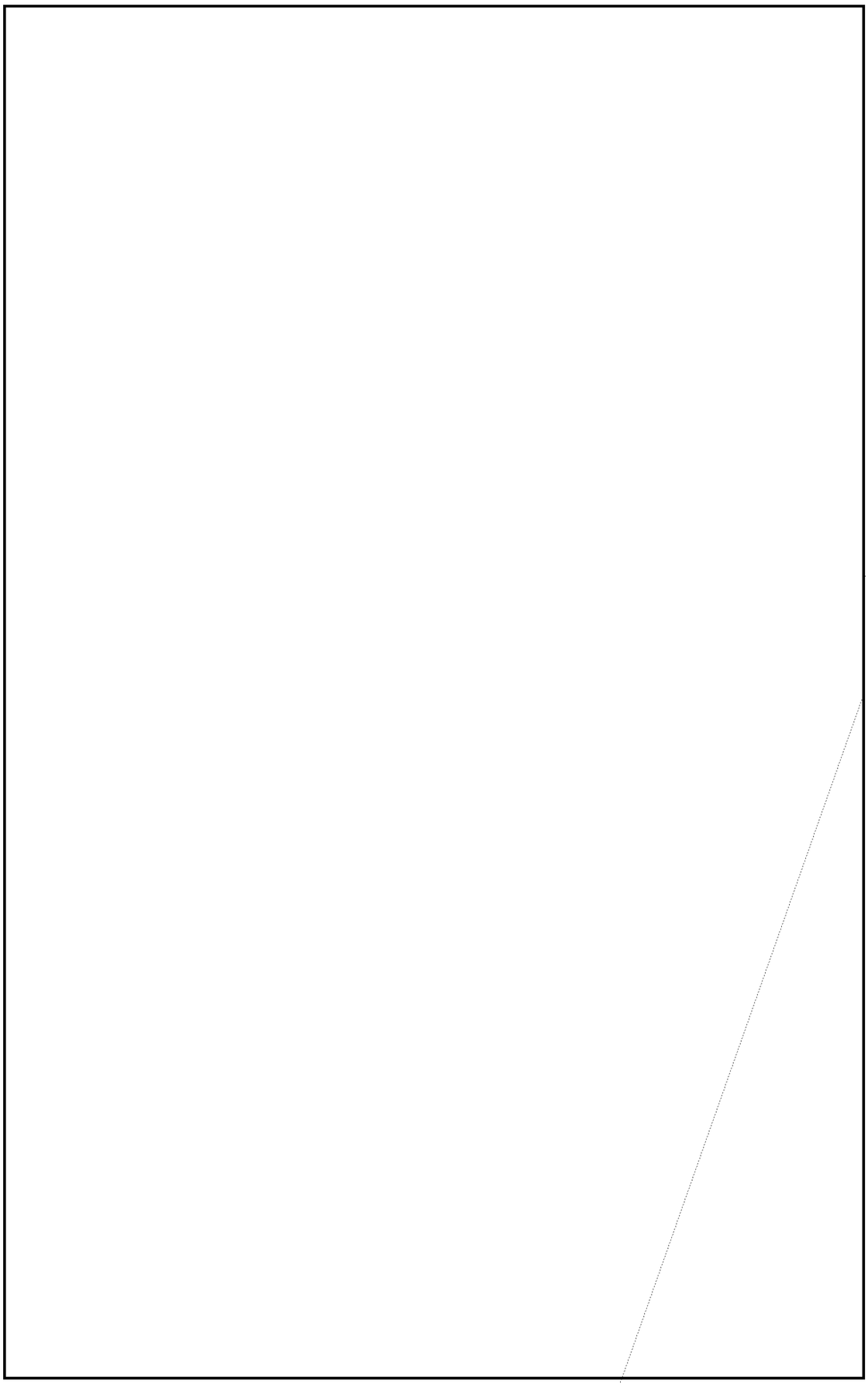
b. Forward a list of examples of dangerous cryptographic and communications practices and procedures. This list will be finally

[redacted]

Buffer-flows

11

EO 3.3(h)(2)
PL 86-36/50 USC 3605



EO 3.3(h)(2)
PL 86-36/50 USC 3605

24. The approach described above involves complicated issues which raise intelligence and political, as well as communications security, problems. These will require special attention and rapid coordination between the US and UK until the precise direction and success of this program have been assured. Among the several liaison arrangements which exist now in these fields there does not exist the specific informal mechanism which would afford the representation and flexibility required for this purpose. additional

CONCLUSIONS

[redacted]

source of highly valuable intelligence for the USSR.

[redacted]

authoritative intelligence of high value through other sources of information.

[redacted]

country might defect from the NATO Alliance is not estimated to affect the validity of this conclusion.

28. Action should be taken immediately to rectify all vulnerable communications security practices of NATO countries.

29. Intelligence and security considerations require that any remedial action taken, while designed to be effective, possible [redacted] non-NATO nations.

30. Certain technical factors and general considerations require that the action taken should:

a. Attack violation of NATO communications security regulations through improvement of the overall communication security attitudes and practices of offending NATO countries.

b. [redacted]

c. Utilize the machinery of the Standing Group of NATO as the instrumentality for improving the security of the national communications of other NATO countries.

d. Be taken through communications security channels, using existing communications security agencies wherever possible.

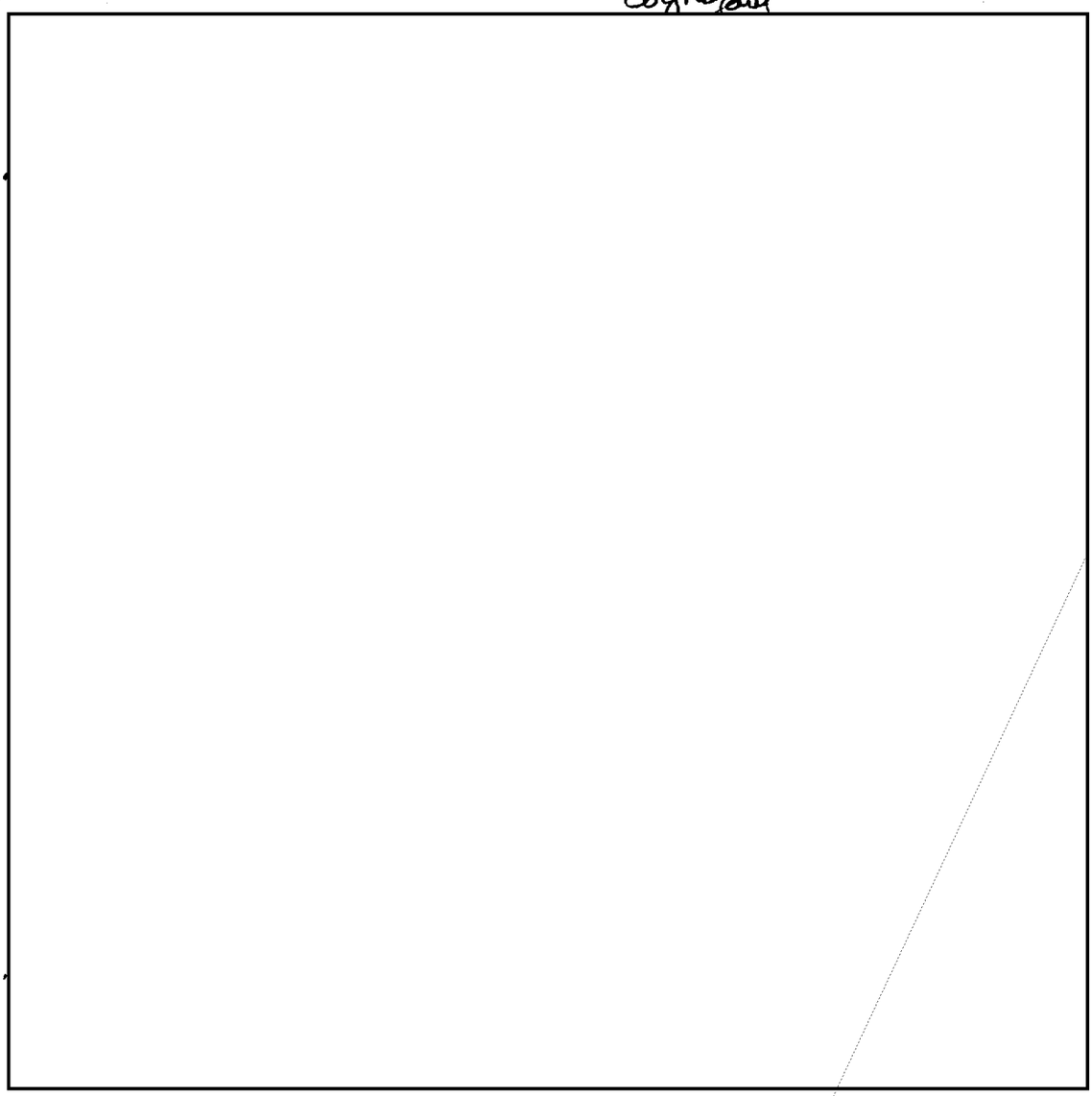
e. Be aimed at the improvement of available cryptosystems and communications practices wherever possible, rather than at the provision of new equipment.

f. Afford maximum privacy in dealing with individual NATO countries.

31. The course of action outlined in paragraphs 18 thru 24 above meets the foregoing considerations and is feasible.

32. Upon approval of this Report paper the following preliminary steps must be taken:

cognizant



drawing of lessons from it are adequate, and no further liaison machinery is required.

RECOMMENDATIONS

34. It is recommended that:

a. The foregoing conclusions be approved and supersede those of the 1951 UK-US Conference on the Security of [redacted] Communications.

b. The program in paragraphs 18 through 24 be undertaken in accordance with the conclusions and, in particular, that the steps enumerated in paragraph 32 should be undertaken immediately.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

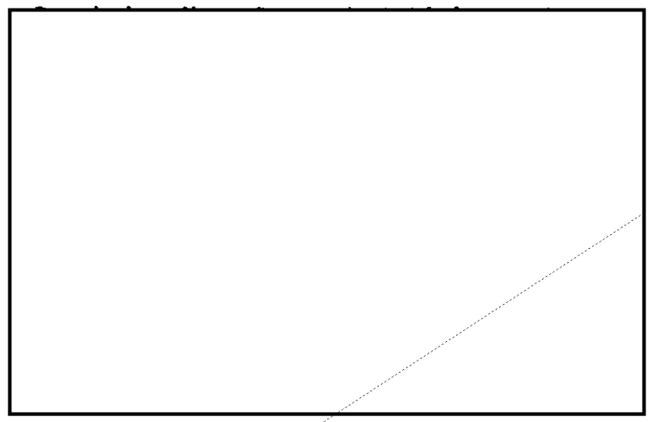
~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R(2)
010

12 June 1953

APPENDIX A

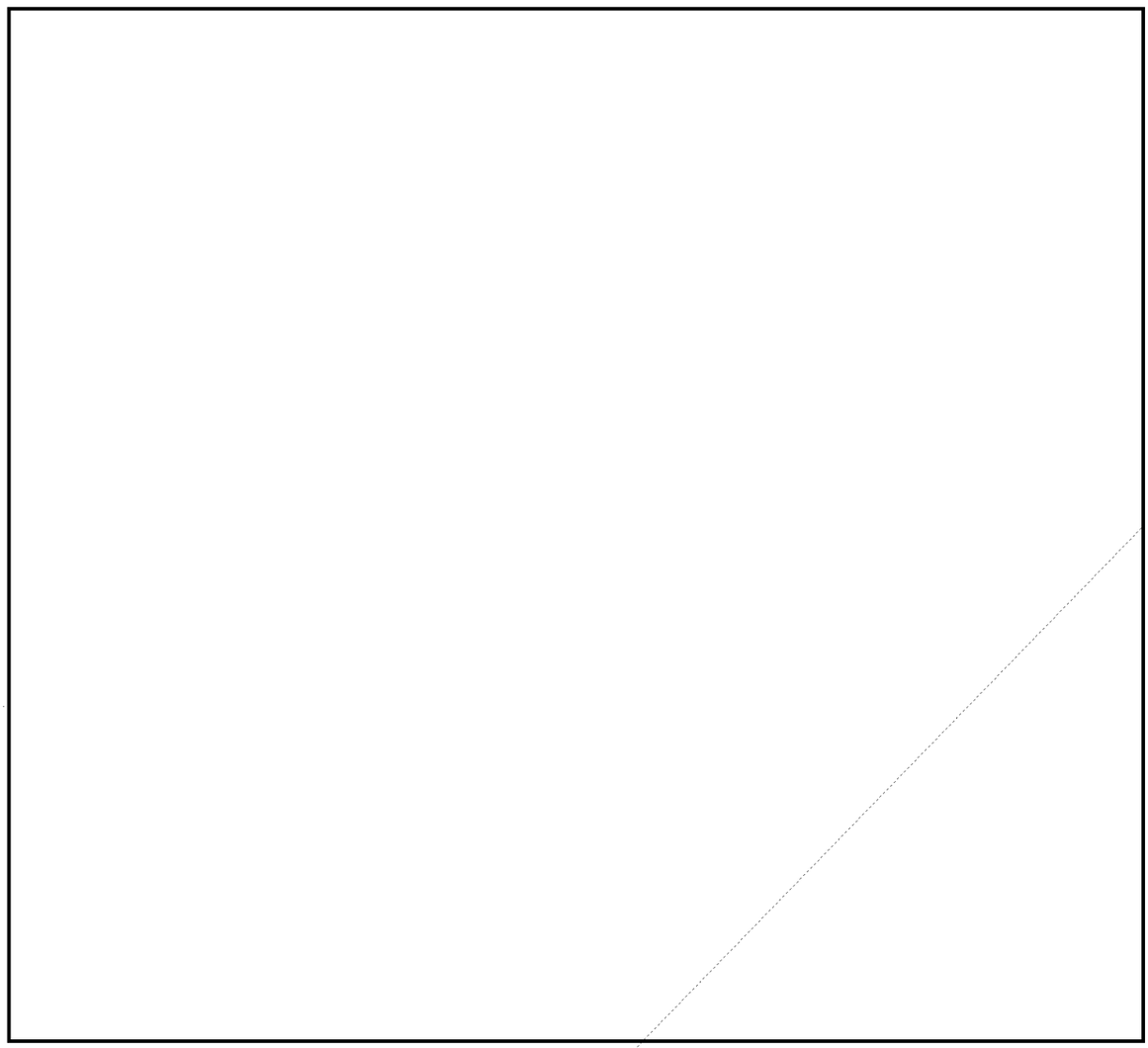
Examples of Recent Instances in which NATO



EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET CANOE - SECURITY INFORMATION~~

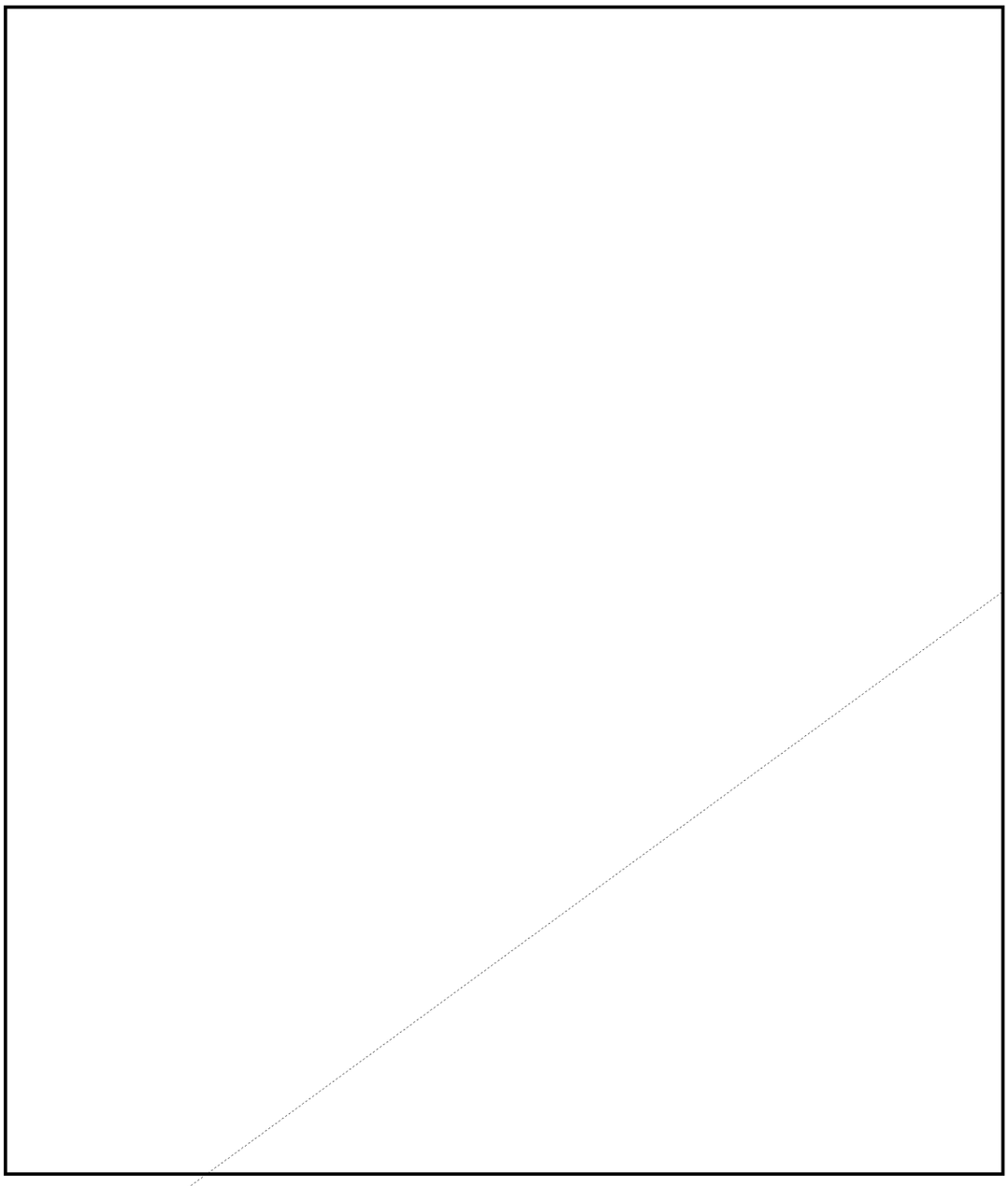
FSC53/EX/R(2)
010



EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R(2)
010



EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET CANOE~~ - ~~SECURITY INFORMATION~~

FSC53/EX/R(2)
010

12 June 1953

APPENDIX B

LIST OF EXAMPLES OF DANGEROUS CRYPTOGRAPHIC AND COMMUNICATIONS PRACTICES AND PROCEDURES

I. UNENCIPHERED CODES

1. Unenciphered codes are totally inacceptable in diplomatic use for transmission of classified information. In Armed Forces communications they are acceptable only when changed at very frequent intervals and when it is not considered essential to maintain the security of the information for more than two or three days from the introduction of the code.

II. ADDITIVE SYSTEMS

2. Any additive (or subtractor or minuend) system is dangerous unless special precautions are taken in the construction of the additive itself. Many procedures that may be regarded ~~by the professional cryptographer~~ as "special precautions" are deceptive as to security and may even in themselves create weaknesses.

3. Encipherment by additive can only be guaranteed to be secure when the additive is used on a strictly "one-time" basis, and systems that permit depth gain little or no security from the additive.

4. Encipherment by non-one-time additive is highly dangerous, but can be acceptable in certain circumstances for limited traffic provided that precautions are taken to minimise overlap and to prevent cryptanalysts from finding any overlap that may arise.

III. NON-ADDITIVE HAND SYSTEMS

5. ~~Encipherment by hand methods other than additive can seldom~~ are many be guaranteed to be secure.

IV. MACHINE CIPHERS

6. Machine ciphers vary greatly in the amount of security they afford. Failure to observe in every detail proper instructions for

operation may lead to compromise even with the best machines. Others, such as the well-known [redacted] are insecure unless precautions are taken over and above those recommended by the manufacturer. Others, again, are basically insecure and should in no circumstances be used.

[redacted]

c. With proper precautions this machine can give very good security for a limited amount of traffic, but in view of the number of different dangers that can arise in varying conditions of use, for which it is impossible to legislate in advance, member nations who wish to make use of the [redacted]

V. TRANSMISSION SECURITY

8. Ciphers, however good individually, are not enough to ensure communications security. Transmission techniques and message formats can in themselves provide considerable intelligence to a traffic analyst. Although there are practical limitations, the ideal to be striven for is that the traffic neither of any one type (e.g. naval, air force,

etc.), nor of any one nation should be distinguishable by external characteristics. Again, intelligence can be gained by study of the organization and procedure of radio networks and by use of radio direction-finding. In many cases, especially in Armed Forces communications, a skillful enemy can obtain valuable intelligence by collation of apparently uninformative ~~plain language~~ messages. It follows, therefore, that full communications security demands that special precautions be observed in such matters as the judicious employment of indicators, the selection of callsigns and of frequencies, radio procedures, and the restriction of the use of plain language.