

~~TOP SECRET~~~~CANOE~~

99

~~TOP SECRET CANOE - SECURITY INFORMATION~~

REPORT

TO

THE LONDON SIGNAL INTELLIGENCE BOARD

AND

THE UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD

ON

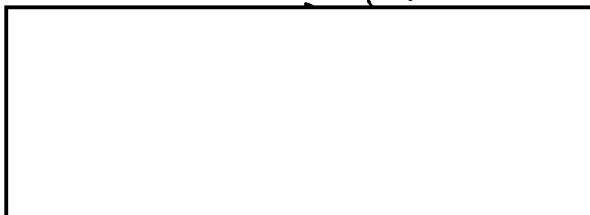
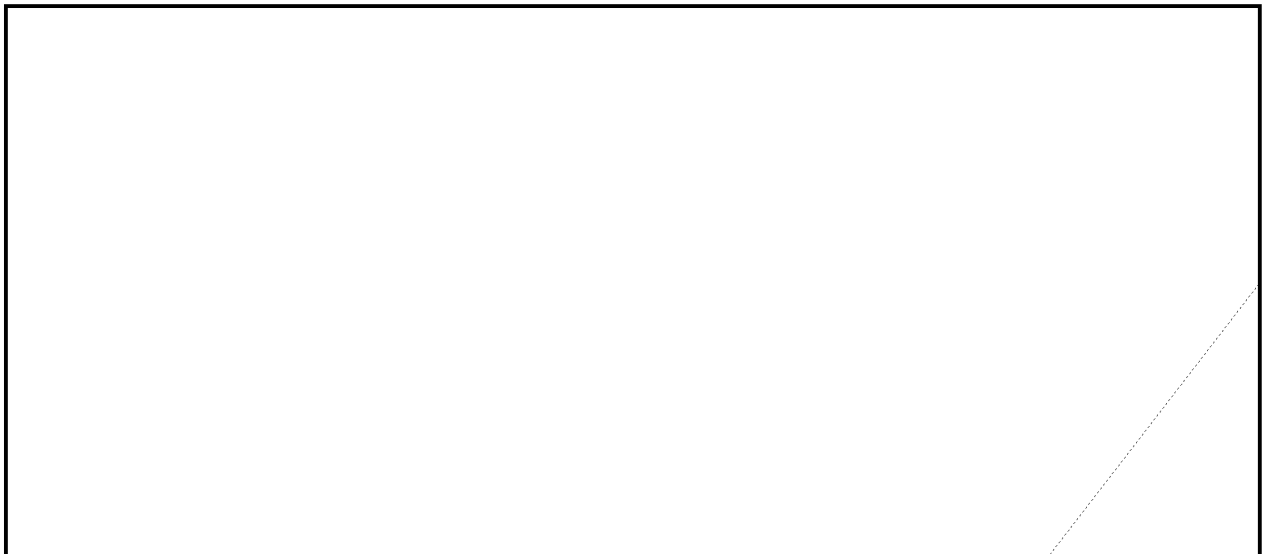
THE U.K.-U.S. CONFERENCE ON THE COMMUNICATIONS SECURITY OF
NATO COUNTRIES

HELD AT WASHINGTON, D. C. - 5-12 JUNE 1953

1. As the result of an LSIB proposal of 26 February 1953,* and the USCIB acceptance thereof, communicated to LSIB by letter dated 18 April 1953,** a UK-US Conference to consider the improvement of the communications security of NATO countries was held in Washington commencing the 5th of June, 1953.

2. The detailed conclusions and recommendations of the Conference, which were agreed by the conferees at their final meeting on the 12th of June, 1953, and which are set forth in the accompanying report, are submitted for approval by the London Signal Intelligence Board and the United States Communications Intelligence Board.

3. Both Delegations recommend that a copy of the Report be forwarded



William F. Friedman

WILLIAM F. FRIEDMAN
Chairman, U.S. Delegates

*DGC/3242
**CIB/00045

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

Declassified and approved for release by NSA on 02-26-2014 pursuant to E.O. 13526

~~TOP SECRET CANOE~~

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

ECS53/UK/W. P. HILL /

011

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

12 June 1953

REPORT OF THEUK-US CONFERENCE ON THE COMMUNICATIONS SECURITY OF
NATO COUNTRIESHELD IN WASHINGTON, 5-12 JUNE, 1953THE 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 Communications, in order:

- a. To determine whether the NATO Governments should be approached with a view to improving their communications security;
- b. To assess the advantages and disadvantages of such an approach;
- 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 DISCUSSIONI. ASSUMPTIONS AS TO THE COMINT CAPABILITY OF THE USSR

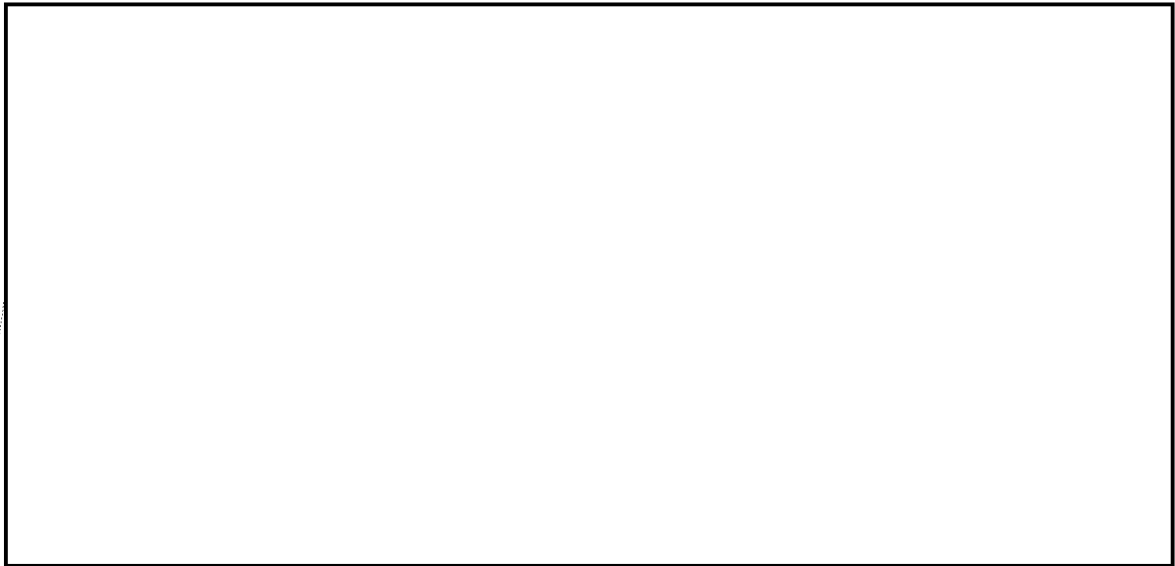
2. This Report is predicated upon the assumption that:
 - a. The capabilities of the USSR to intercept and exploit radio communications are at least equivalent to those of the US and UK.
 - b. The USSR monitors all landline communications passing through its own or satellite territory. The possibility 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.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE - SECURITY INFORMATION~~

EGCSB/EX/R FINAL
011



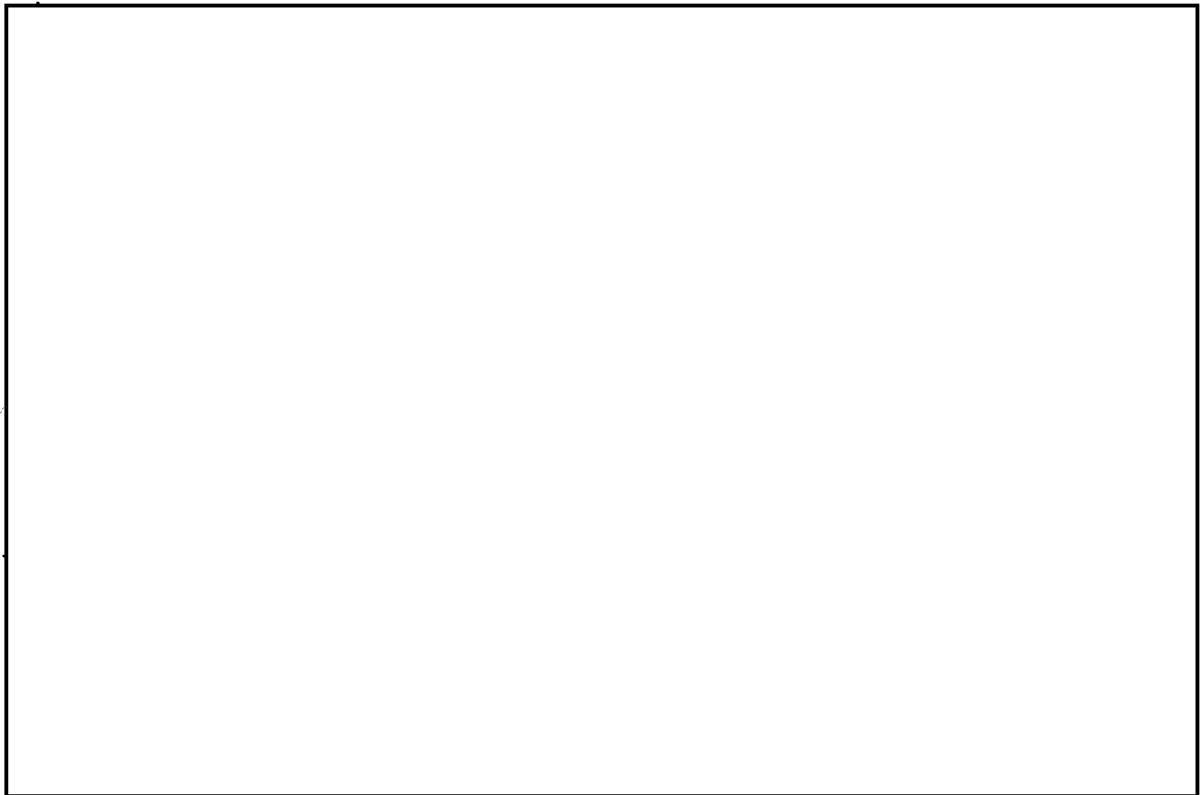
Footnote 1.

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



fully complied with these regulations. There is no evidence on which to conclude whether or not other NATO countries observe the NATO procedures.

Footnote 2.



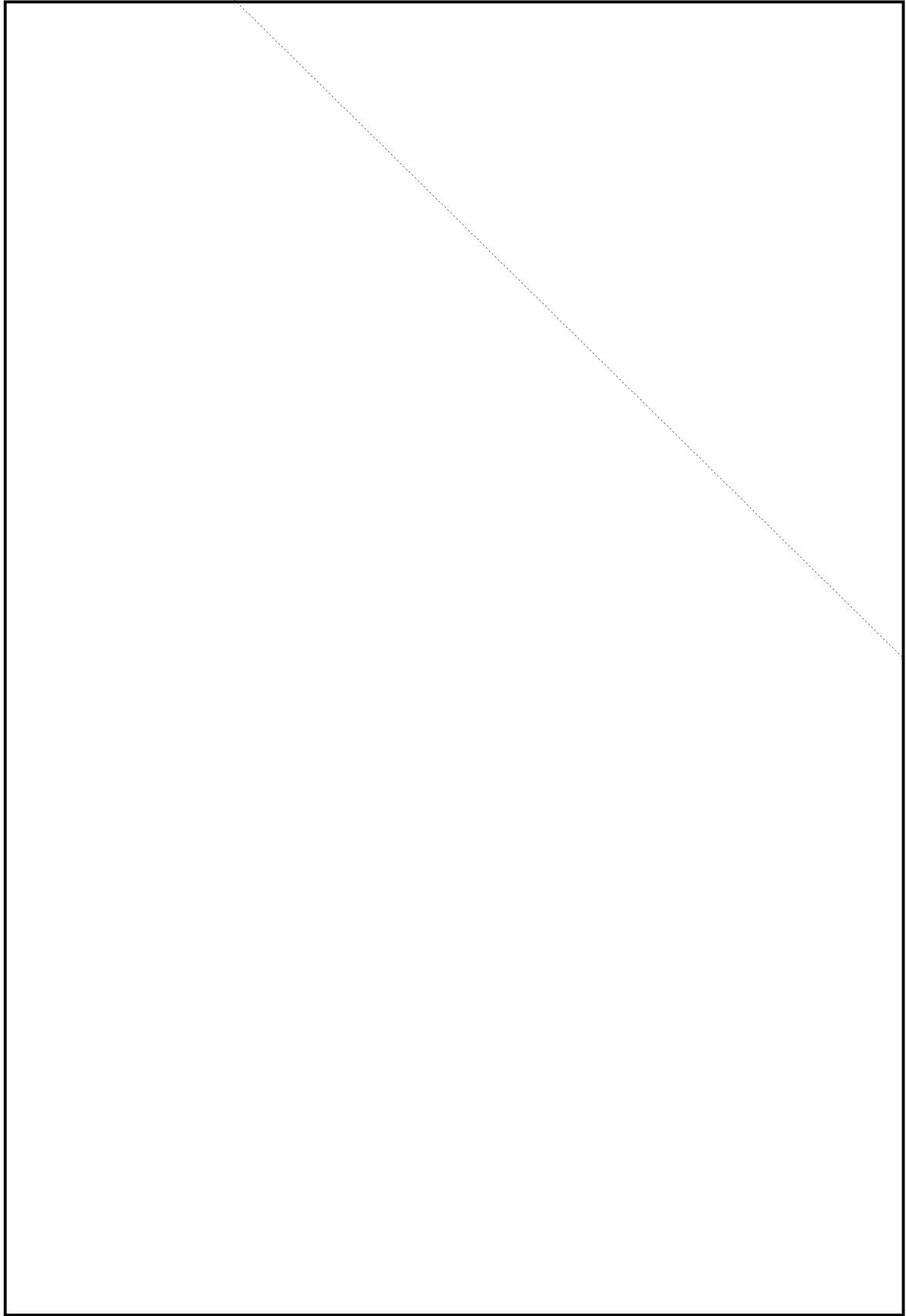
~~TOP SECRET CANOE~~

~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R FINAL

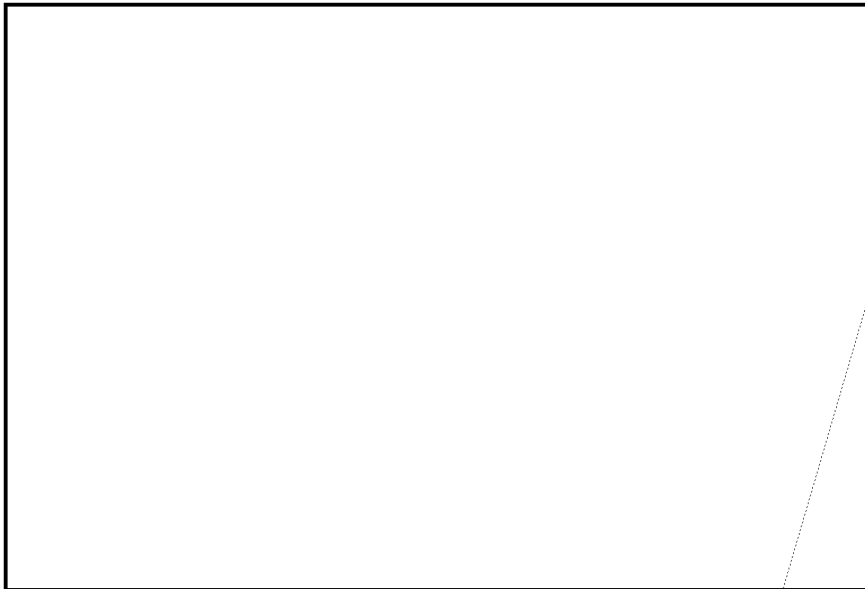
EO 3.3(h)(2)
PL 86-36/50 USC 3605

011




~~TOP SECRET CANOE~~~~TOP SECRET CANOE - SECURITY INFORMATION~~FSC53/EX/R FINAL
011

(5)

4. Diplomatic 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 communications in peace and war.

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,  it is, however, considered that vulnerable Armed Forces 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.

EO 3.3(h)(2)
PL 86-36/50 USC 3605~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE SECURITY INFORMATION~~FSC53/EX/R FINAL
011

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 by the user agency. Further, the 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,

~~TOP SECRET CANOE~~

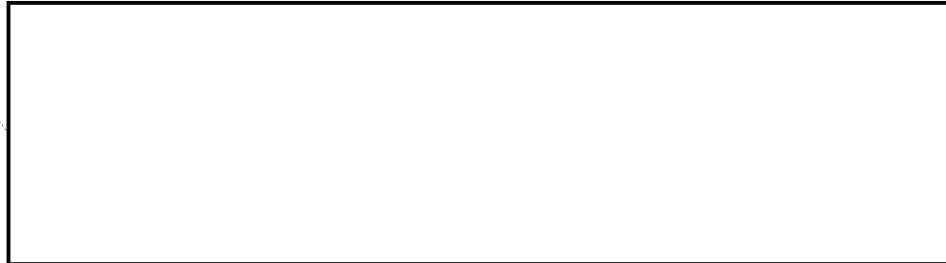
~~TOP SECRET CANOE~~

EO 3.3(h)(2)

PL 86-36/50 USC 3605

~~TOP SECRET CANOE - SECURITY INFORMATION~~FSC53/EX/R FINAL
011

Security Survey of December, 1952, and there remain significant handicaps--political and administrative--to improvement. The level of overall security 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 not available any



evidence it is not considered safe to assume that the level of overall security is higher than that of [redacted] as described above.

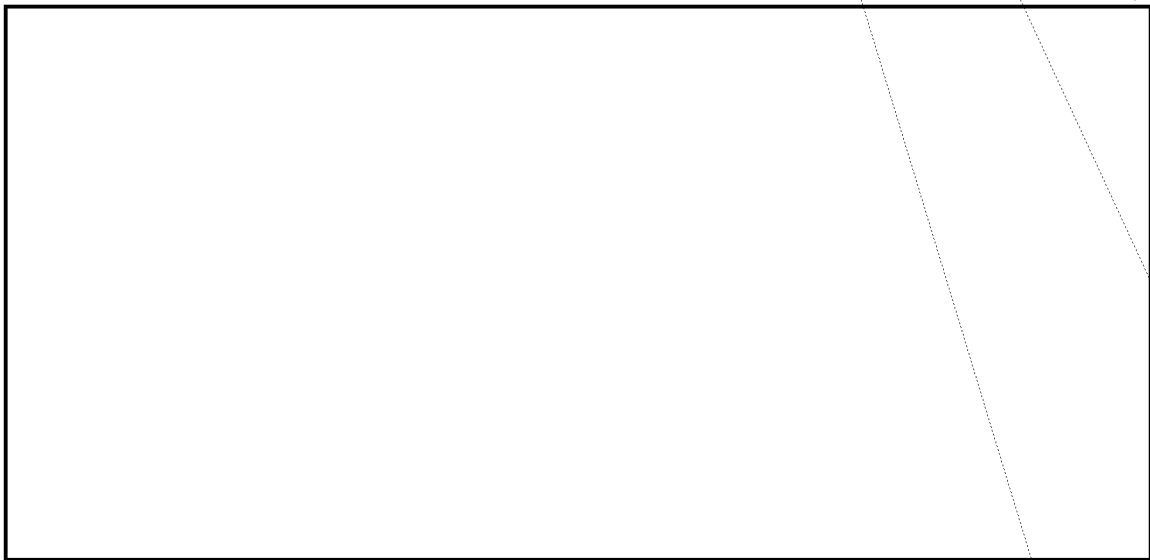
c. In time of war, due to the introduction of security measures which are not possible in peacetime, clandestine operations become much more difficult. The ready means of communication afforded by diplomatic missions and consulates are also no longer available. It is therefore considered that the value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

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE - SECURITY INFORMATION~~EGG53/EX/G FINAL
011EO 3.3(h)(2)
PL 86-36/50 USC 36057. Other Sources

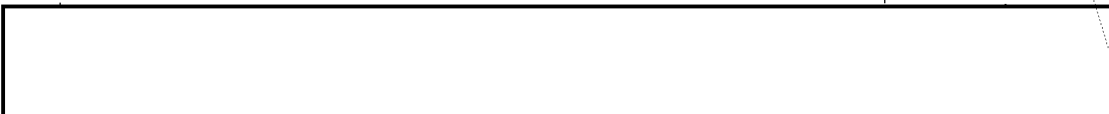
a. It is difficult to assess to what extent open sources (newspapers, trade publications, public documents and statements, etc.) or diplomatic reportage could be a substitute for COMINT. It is however agreed that COMINT derived from readable communications of NATO countries does produce intelligence not available to the USSR from other 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.



consideration the availability of other sources of the same intelligence open to the US and the UK.

9. In addition it should be noted that, if a country left



not be a factor if the country joined the Communist Bloc, since it is to be expected that its ciphers and communications procedures would then be radically improved in any case.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE - SECURITY INFORMATION~~

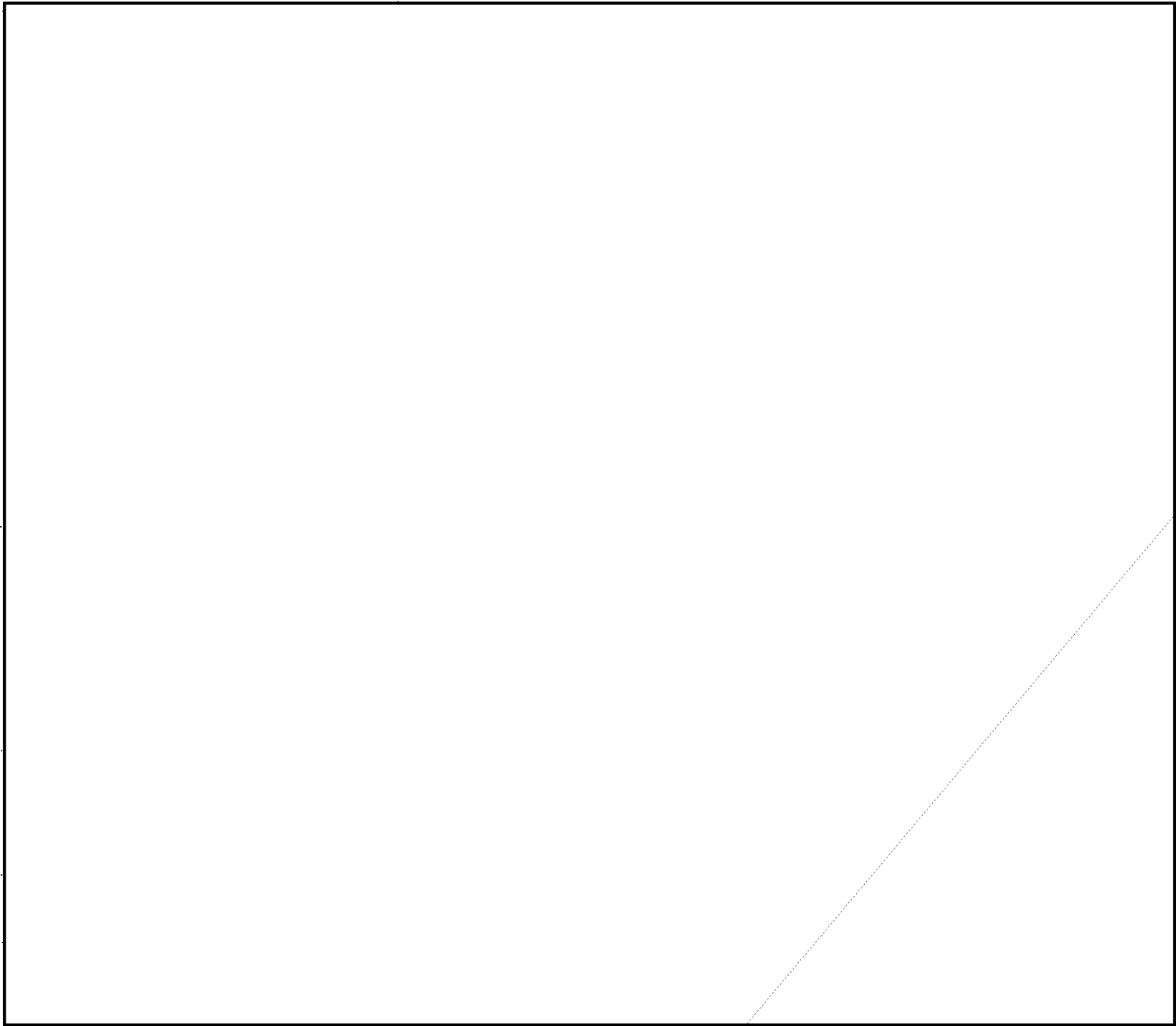
NSC53/EX/R FINAL
011

V. SECURITY AND INTELLIGENCE FACTORS AFFECTING ACTION TO BE TAKEN

*Security factors
considerations
action to be taken*

10. The nature of any action taken to reduce the potential damage to the national security of the 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.



~~TOP SECRET CANOE~~

VI. TECHNICAL FACTORS AFFECTING ACTION TO BE TAKEN.

1. 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.

2. 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 be used wherever possible. At least the US, UK and the Standing Group have already in existence appropriate communications security agencies.

c. There have already been several instances in which NATO countries have requested advice and assistance in improving national, as well as NATO, communications security through communications security channels. Two examples of such instances are enclosed herewith as Appendix A.

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

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



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R FINAL
011

VII. OUTLINE OF THE PROPOSED ACTION.

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.

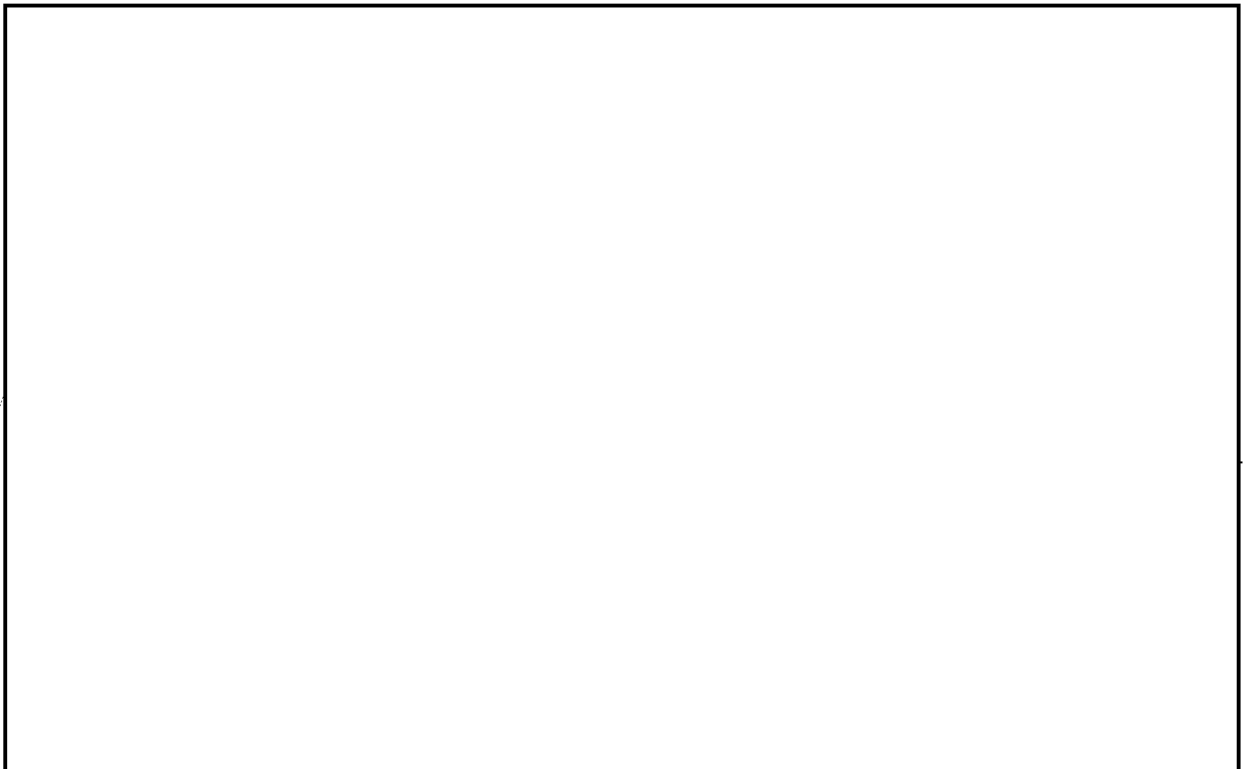


2

17. In order to avoid embarrassment, to ensure maximum cooperation, and to adhere to the security and intelligence factors enumerated in paragraph 10 above, any action with an individual country should be as inconspicuous and private as possible.

3

VIII. THE DETAILED APPROACH AND SUBSEQUENT ACTION.

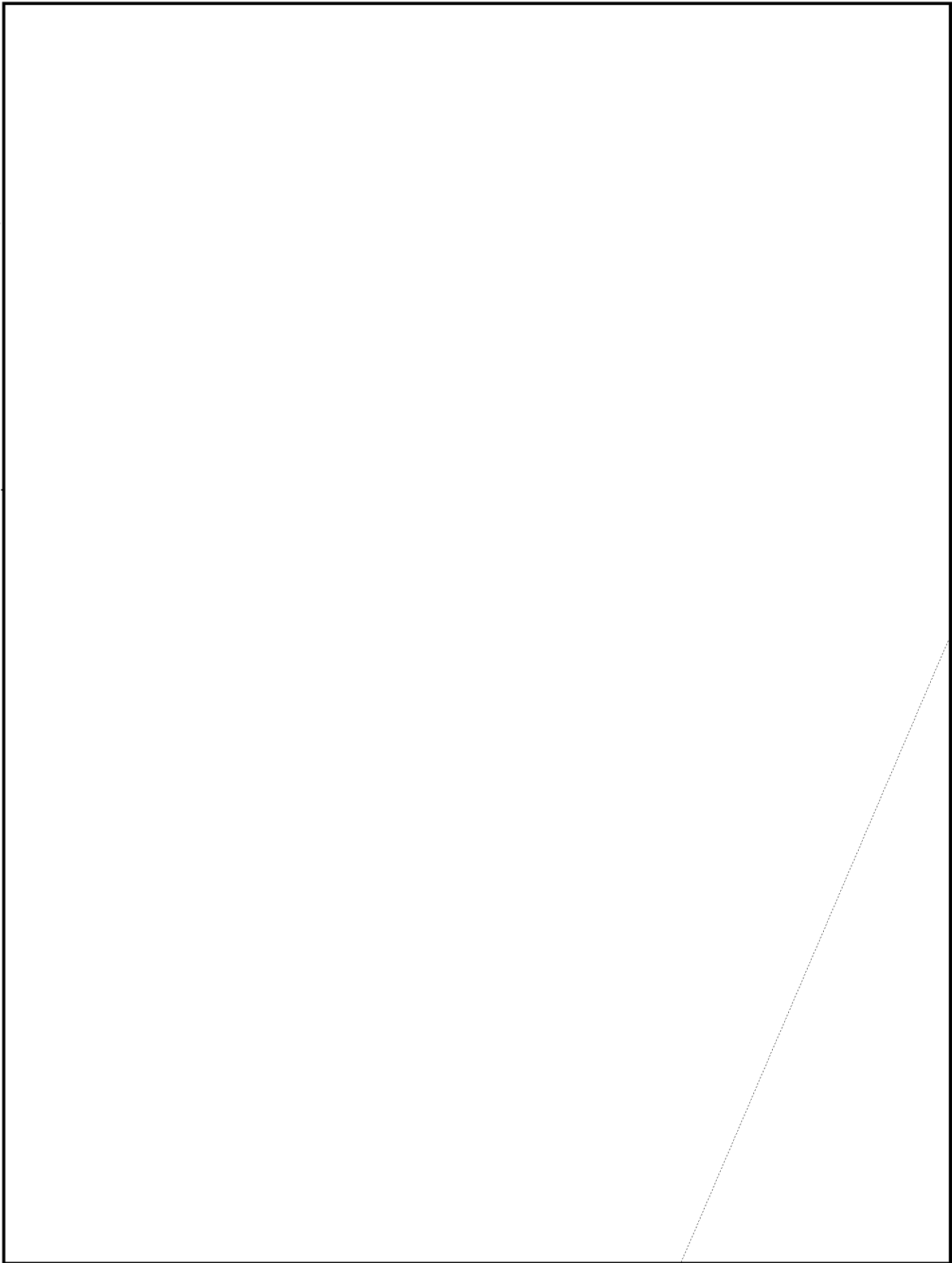


1

steps to improve their communication security.

~~TOP SECRET CANOE~~

2



~~TOP SECRET CANOE~~

~~TOP SECRET CANOE - SECURITY INFORMATION~~

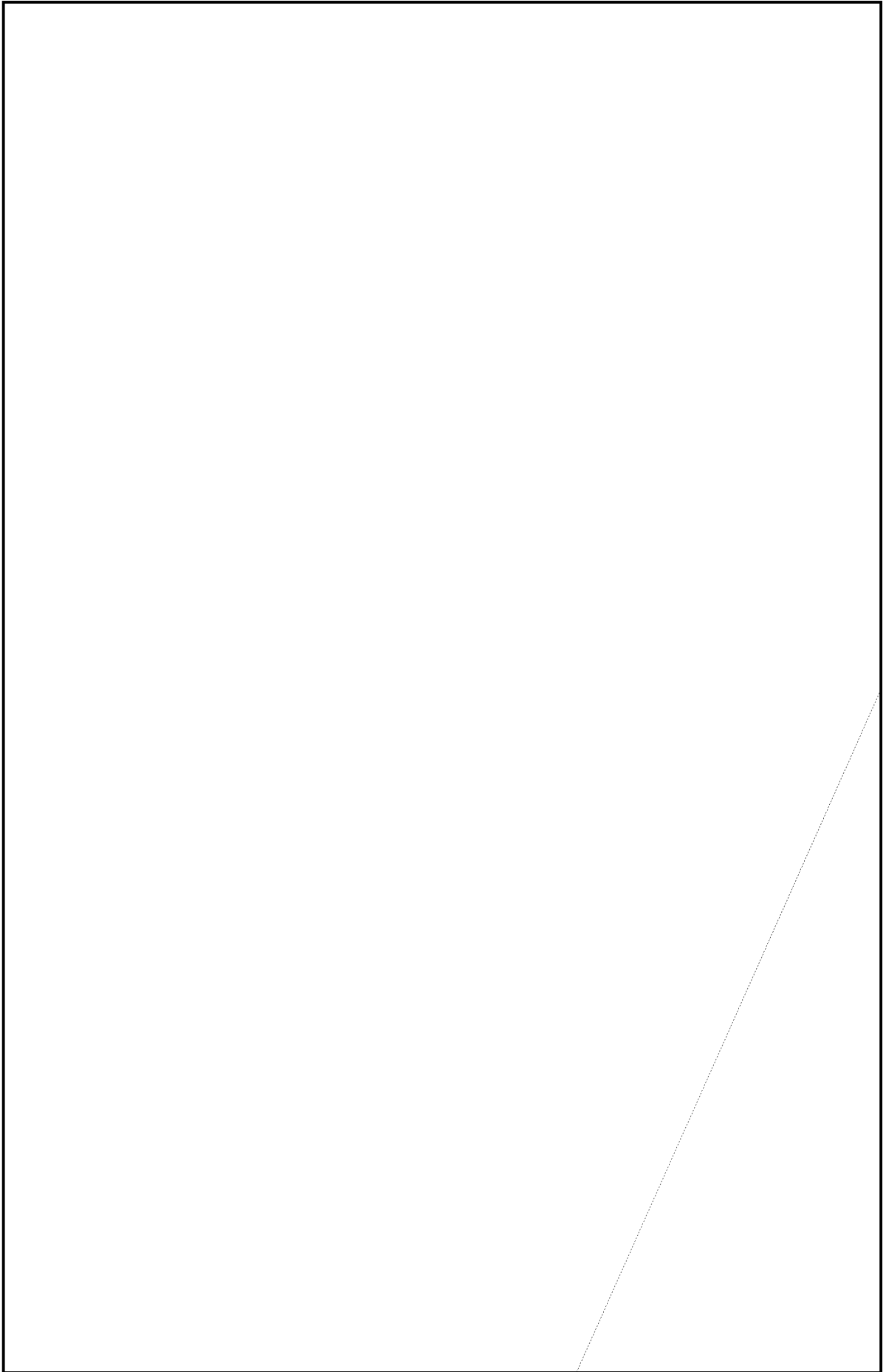
83053/EX/R FINAL
011

3

4

5

6



~~TOP SECRET CANOE~~

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

~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R FINAL
011

4. 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. It is considered that the need would be met by the setting up in Washington of a small combined working group representing intelligence and political as well as technical interests, the exact composition and terms of reference to be decided by consultation between the cognizant US and UK authorities.

CONCLUSIONS

[Redacted]

what extent national armed forces ciphers of NATO countries are vulnerable. If vulnerable however they also constitute a potential source of highly valuable intelligence for the USSR.

[Redacted]

2
adequately for the loss of COMINT as a potential source of timely and authoritative intelligence of high value through other sources of information.

[Redacted]

3
The possibility that any NATO country might defect from the NATO Alliance is not estimated to affect the validity of this conclusion.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE SECURITY INFORMATION~~

FSC53/EX/R FINAL
011

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, should not



actions taken should be calculated to prevent the leakage of effective communications security principles to 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.

P11



P16

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.

Tab 15
19

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

P12

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

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

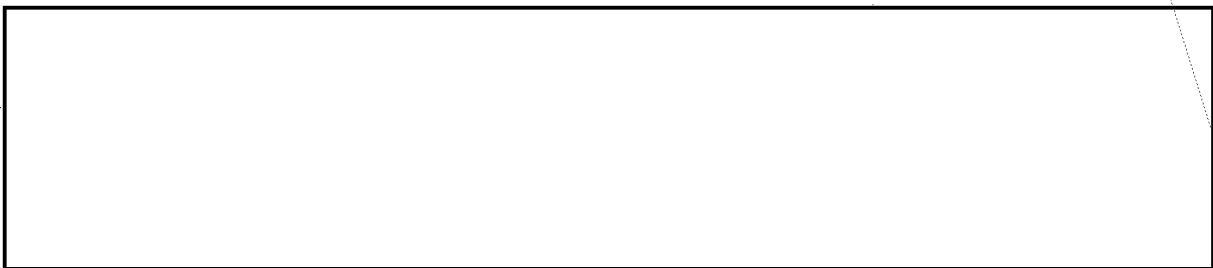
~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R FINAL
011

6 | f. Afford maximum privacy in dealing with individual NATO
countries. EO 3.3(h)(2)
PL 86-36/50 USC 3605

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

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



liaison arrangements to coordinate this examination and the drawing
of lessons from it are adequate, and no further liaison machinery is
required.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE SECURITY INFORMATION~~FSC53/EX/R FINAL
011RECOMMENDATIONS

34. It is recommended that:

a. The foregoing conclusions be approved and supersede those of the 1951 Conference on the Security of 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~~

~~TOP SECRET CANOE~~

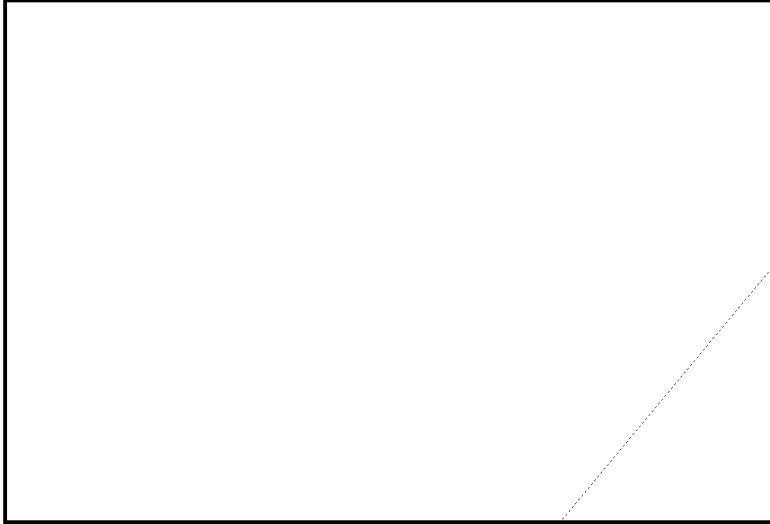
~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R FINAL
011.

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~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R FINAL
011



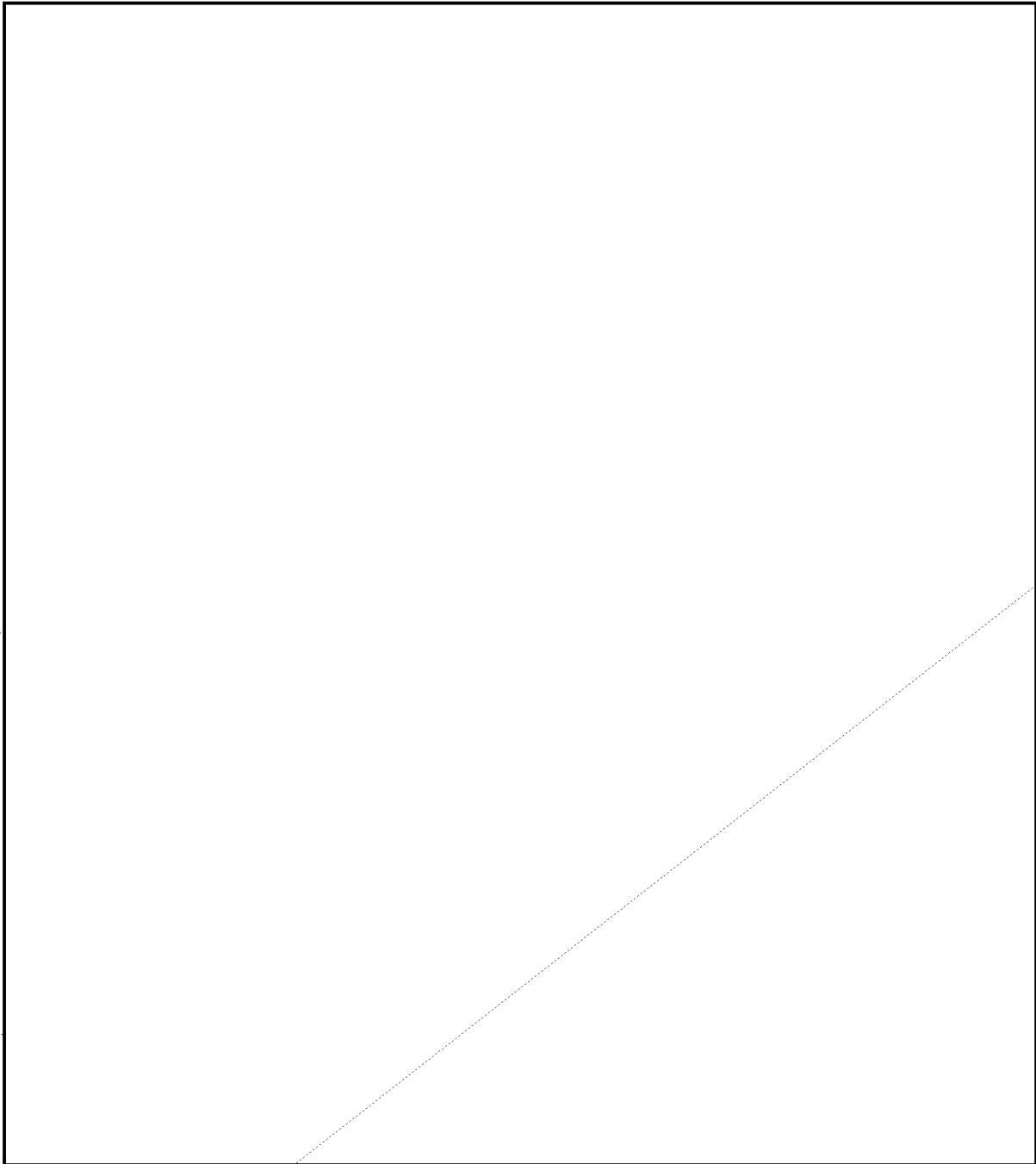
EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R FINAL
011



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

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE - SECURITY INFORMATION~~FSC53/EX/R FINAL
011

12 June 1953

APPENDIX BLIST OF EXAMPLES OF DANGEROUS
CRYPTOGRAPHIC AND COMMUNICATIONS
PRACTICES AND PROCEDURES

I. UNENCIPHERED CODES

1. Unenciphered codes are totally unacceptable 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 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 additives is highly dangerous, but can be acceptable in certain circumstances for limited traffic provided that precautions are taken to minimize overlap and to prevent cryptanalysts from finding any overlap that may arise.

III. NON-ADDITIVE HAND SYSTEMS

5. There are many hand methods of encipherment, not employing additive, but few of these can 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

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE SECURITY INFORMATION~~FSC53/EX/R/FINAL
OLIEO 3.3(h)(2)
PL 86-36/50 USC 3605

12 June 1953

APPENDIX B(continued)

operation may lead to compromise even with the best machines.

Others, such as the well-known

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.

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,

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~~~TOP SECRET CANOE - SECURITY INFORMATION~~RSC53/EX/R FINAL
011

12 June 1953

APPENDIX B (continued)

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 message texts. 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 call signs and of frequencies; radio procedures, and the restriction of the use of plain language.

~~TOP SECRET CANOE~~