USCIB: 23/57

APPENDED DOCUMENTS CONTAIN CODE WORD MATERIAL

27 May 1953

~~TOP SECRET~~ - SECURITY INFORMATION

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Allied (NATO) Communications Security.

1. The enclosed [redacted] position paper on the subject of NATO Communications Security is forwarded for information and study.

2. The [redacted] has informed the Secretariat that, although the paper has been approved by [redacted] without amendment, it should be considered as an informal statement of the views of the Director, [redacted] at this time.

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

RJ Karl
for RUFUS L. TAYLOR
Captain, U. S. Navy
Executive Secretary, USCIB

Enclosure
DGC/3441 dtd
20 May 1953.

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

INTRO

DGC/3441

20th May, 1953

Copy No.: ~~........~~

SECURITY OF THE [redacted] OF THE NATO POWERS

Intro

INTRODUCTION

The present paper contains a review of the situation with [redacted] recommendations on the extent of the remedial action required and on the methods to be adopted to convince the governments concerned of the need for action, without disclosing sophisticated cryptanalytic techniques.

The [redacted] views are summarised in the following paragraphs:-

It is the [redacted] view that at the present time ① the insecurity of the [redacted] is of considerably more value to the Russians than it is to U.K. and U.S., ② and that were this source of leakage removed the Russians could not obtain the same information by physical means. In war leakage of this kind would be even more damaging to [redacted] interests and profitable to the Russians owing to great increase in quality and quantity of the telecommunications of friendly powers, and the increased difficulty of obtaining information by non-Comint means. Appendix 'A' to this paper contains a survey made at [redacted] with annexures giving recent examples of information, of value to Russia, passed by [redacted] powers in [redacted] Appendix 'B' contains some examples, taken from [redacted] War Histories, showing the kind of damage which the Axis powers did to one another by use of [redacted] as well as the damage suffered by the Allies from the insecure communications of the [redacted]

Proof ? 2,
Proof ? 7,

[redacted]

① No up-to-date evidence is available on the state of [redacted] of any [redacted], but it may be presumed that the [redacted] [redacted] of all the countries listed above are more or less insecure, and in as much need of remedial action as the same countries' [redacted] systems. ② It is also desirable in the [redacted] view to seek information on the [redacted] although the [redacted] of these countries appear to be satisfactory.

The [redacted] view is that ① the problem is one for discussion among communication security officers, and ② that it is essential for [redacted] to substantiate their case for improvement of [redacted] by drawing attention to weaknesses which they have found to exist, but ③ quite unnecessary and indeed irrelevant to describe the techniques of cryptanalysis used in exploiting these weaknesses.

Low?

[redacted]

Who [redacted] ?

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

DGC/3441

Appendix 'C' contains some examples taken from a modern [redacted] work on cryptanalysis showing that in telling the [redacted] that their cyphers are in principle usound we shall be telling them nothing that they do not already know.

Finally it is the [redacted] view that having taken steps to improve [redacted] the three powers should form a tripartite committee which would deal with other members of [redacted] on similar lines.

DGC/34M

Report

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

REPORT

I

SCOPE OF THE PROBLEM

(a) [redacted]

1. It was agreed at the [redacted] Conference of May 1951 that it was in the common interest to render [redacted] secure against [redacted] attack.

2. A reservation was made in respect of the [redacted] for the following reasons:

(i) that no likelihood existed of the [redacted] extending its use to radio channels;

(ii) that our knowledge of the existence of the machine was derived solely from "clandestine" sources, and

(iii) that sophisticated techniques, that must not be disclosed to the [redacted], were used in exploiting it.

3. The [redacted] have meanwhile begun to use the machine on some radio channels and intend to use it on others. This disposes of the first objection, and to some extent also of the second, since the "clandestine" source referred to was simply the monitoring in [redacted] of a [redacted] from the [redacted] The approach described in the present paper is designed to avoid any necessity for disclosure of sophisticated techniques. It is therefore considered desirable that the [redacted] be included in any discussions with the [redacted]

(b) [redacted]

4. The [redacted] Conference of May 1951 considered and rejected a proposal to take action to improve the security of [redacted] cyphers for two reasons:

"(i) the [redacted] through the mechanism of NATO and without revelation of Comint, have initiated action which is expected to correct in large measure ~~the~~ insecurity of the important cryptocommunications of the [redacted] and

(ii) any correction of the remaining important areas of insecurity of the cryptocommunications of the [redacted] [redacted] would involve disclosure of success in sophisticated cryptanalysis and possibly lead to a demand for revelation of techniques, both of which revelations must be avoided."

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

5. Although considerable progress has been made since 1951 in the provision of NATO cyphers, the [redacted] show little sign of improvement.(i)

What does G-2 USA say?

(i) [redacted] in [redacted] are wide open from the highest level downwards and carry a large volume of intelligence that is damaging not only to the [redacted] themselves but also the their allies; for example, they contain revelations of [redacted] capable of ruining not only the [redacted] against the Viet Minh but also that of [redacted], and they give details of forthcoming American Aid. (see Appendix 'A', Annexure 3.

(ii) "Third level" communications of NATO forces are sent entirely in national cyphers. The content of messages passed at this level may be less immediately revealing than that passed at higher levels, but (in war certainly and probably also in peace) could be treated by "inferential" and "fusion" methods and made to yield valuable intelligence not available to an enemy by any non-Sigint means.

[redacted]

(c) [redacted]

7. The general question of improvement of the national cyphers of the other NATO powers has never been discussed officially between [redacted] [redacted]

(i) The U.S. view on this subject in 1951 was however indicated by the following statement made by an ad hoc committee of U.S.C.I.B. during unofficial discussions arising from use by [redacted] of [redacted] to discuss NATO matters.

"Remedial action involving the entire body of [redacted] communications is not necessary from the point of view of [redacted] in fact it would be undesirable from the point of view of conserving for the U.S. this and other important [redacted]"(ii)

US Ad Hoc Com "dictum" What we ought to do was to get Port to use auth systems for COSMIC

(ii) It was ultimately agreed that the U.S. Government should make a high level approach designed to "shock" the [redacted] into using the [redacted] without however actually revealing that their own cyphers were insecure.

(i) There appears to be some tendency to increase the use of one-time pads but we have no guarantee that the pads are properly made or even that the usage is truly "one time".

(ii) Report of U.S.C.I.B. ad hoc Committee on [redacted] Communication Security, September, 1951.

EO 3.3(h)(2)

(iii) A demarche was made by the U.S. Ambassador to [redacted] in spite of which [redacted] are still a [redacted] (See Appendix A annexure 6).

Different from view at NSA Grp.

8. The [redacted] view is "shock tactics" of this kind are unlikely to be effective especially when they are accompanied by a "cover story" which is unlikely to be believed; the only way to achieve improvement in security habits is by educative action and by influence of the "public opinion" (if such a term may properly be used of a very secret subject) of other powers' [redacted] officers.

9. But the dictum of the U.S.C.I.B. ad hoc Committee referred to in para 7 above has in the [redacted] view another serious weakness in that it is based on the assumption that it is possible in matters of cypher security to "have it both ways". This assumption has appeared at various times in discussion in two different forms:

?

(i) that it is possible to devise cyphers that are just good enough to defeat the Russians but contain weaknesses that can be [redacted] we cannot know anything of the level of competence of U.S.S.R. cryptanalysts.

(ii) that it is sufficient to limit improvement of security to specified cryptochannels or to telegrams on specified subjects. This will not do; it is not possible to forecast in advance which cryptochannels are going to carry important messages and it is not enough to insist on use of [redacted] when documents are [redacted] without also taking steps to protect the security of NATO fringe traffic or national comment on NATO discussions which may legitimately be sent in [redacted]

(d) [redacted]

10. Little is known, from [redacted] sources, of the [redacted] of any European power except [redacted] and if as seems probable they are no better than the [redacted] they would be, in varying degrees, dangerous to the security of any forces operating with them in war.

(e) Cypher machine development in Europe

11. It is known that new cypher machines are being developed by several [redacted] governments and by commercial firms operating in neutral countries.

Olivetti etc

(i) The [redacted] have designed cypher machines which they intend to use for their [redacted] these machines embody some fiarly advanced techniques but from information at present available appear to be most insecure.(1)

(1) See memorandum from [redacted] in Washington to Secretariat of the Standing Group, No. 0927/SRP ~~of 30.4~~.53.

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

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

[redacted]

(ii) The [redacted] are designing random generator for production of one time key ; nothing is known of details.(i)

(iii) The [redacted] in conjunction with a [redacted] firm, is producing a wide range of new cypher machines which will undoubtedly be much better than the same firm's pre-war models, but may still be not secure against modern cryptanalytic methods.

12. This list is probably not exhaustive, and these developments merit close attention from [redacted] While it is entirley possible that European powers may work out their own salvation, with or without the aid of commercial firms, it is to be feared that they may only arrive at an intermediate stage of development when it will become difficult to convince them of their insecurity without revealing too much detail of current [redacted] thought on cypher machine design. It would be therefore better to approach these European powers before their own development has gone too far, and persuade then to adopt well tried [redacted]

(f) Decisions to be taken at the Conference

(A) Countries to be covered

[redacted]

13. A decision has to be taken, one way or the other, in the case of each NATO nation, whether the interests of Signal Intelligence or of Signal Security are to prevail, and no half way house exists. Either we decide to take steps to put that cryptographic house in order, and to sacrifice Signal Intelligence (probably for ever) or we "conserve" the correspondence of that government as a Signal Intelligence target for ourselves - and for the Russians.

(B) Timing of action with relation to physical security

14. The 1951 Conference agreed a limited programme for an approach to the [redacted] on certain [redacted], but recommended no action pending improvement in [redacted] physical security; U.S. have not yet expressed themselves satisfied that such improvement has gone far enough.

15 While it is agreed that we ought to adjust our methods to take account of differing physical security conditions in various countries it may be said

(i) that physical leakages will seldom if ever be so gross as to provide a source of intelligence as rapid, complete, reliable and (above all) authentic as that derived from a major breakdown in communication security; conditions need to be literally hopeless before one can say that there is no point in improving cypher security;

Yes—but suppose R have stolen the keys? Then they can get the authentic info even more quickly than we

(i) Conversation between [redacted] and [redacted] February 1953.

EO 3.3(h)(2)

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

(ii) One should however not delay initiating action on cypher security pending expected improvements in physical security, because neither can be put right overnight.

2

16. The [redacted] recommendation is therefore (1) that there is no case for any further delay in approaching the [redacted] and (2) that physical security of other nations might be considered as a valid reason for taking no action at all, or for taking modified action but not for delaying action.

II

THE APPROACH TO THE [redacted]

17. Having settled the scope of action intended the Conference should, in the U.K. view, consider an approach to the [redacted] with a view to first improving their communications security and then inviting them to associate themselves with any scheme that may have been agreed between [redacted] for approaches to other NATO nations.

18. It is recommended that a single approach be made to the [redacted] covering all cyphers of all services in respect of which ~~the~~ conference has decided that action must be taken.

19. Previous projects for approach to the [redacted] on the delicate subject of the security of [redacted] ~~have~~ been based on the assumption that this insecurity is due to ignorance of the art of cryptography which cannot be removed without exposure of "sophisticated" cryptanalytic techniques. Yet after all, the basic principles of cryptography are few, simple and well known to all cypher experts including the [redacted] and do not constitute the "secret" upon which the success of cryptanalysis depends. The "secrets" of cryptanalysis are rather these:

Why is this a "secret". F. Bacon said in 1590: But surely is the rawness + unskilfulness [illegible] do

(i) that situations arise in the use of cyphers which would instantly be condemned as insecure by any one instructed in cryptography;

(ii) that other situations arise which an instructed person would admit to offer at least a theoretical risk of insecurity, but which require "sophisticated techniques" to exploit them, and that these techniques have been devised.

agree

20. The only way in which improvement in [redacted] can be eventually obtained is by cooperation on the technical level between [redacted] [redacted] communication security officers.

21. The object of the first approach therefore would ~~be to~~ bring about a frank exchange of information that would serve as a basis for

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

subsequent discussion among responsible communication security officers. One of the points that the Conference must decide is whether this initial exchange should be made:

(i) at a tripartite meeting;

(ii) at separate bipartite meetings, [redacted]

(iii) at a single bipartite meeting where either [redacted] would state the whole case against [redacted]

22. The tripartite arrangement would be the best, apart from the fact that it would be impossible to conceal the fact that [redacted] and [redacted] had discussed the matter and exchanged information before the meeting began. The single bipartite meeting would involve either [redacted] or [redacted] in a fairly complicated cover story. If for example [redacted] were to undertake the whole task they would be obliged to make the case on [redacted] entirely from material received from [redacted] Two bipartite meetings seems to make the worst of both worlds, and in any case whether [redacted] cooperation is explicitly admitted or not it will undoubtedly be assumed. It is therefore recommended that the meeting be tripartite.

23. The exchange can be initiated in two ways only:

(i) by inviting each party to describe its own communication security methods, which would then be discussed on general cryptographic grounds by the other two.

[redacted]

(ii) By [redacted] announcing that they are already aware of the existence of security weaknesses in [redacted] communications, describing them and inviting the [redacted] to disclose any knowledge that they may have of [redacted] [redacted] (i)

24. The second approach is recommended, as being more sure of its effect.

(i) Initially at least it may be somewhat embarrassing but it will have less long term disadvantages in that it does not commit anybody to disclosure of details of their own systems which they consider irrelevant or do not wish to mention.

(ii) Although this approach implies a tacit admission of

(i) This is something more than a polite fiction. We already know that the [redacted] have been monitoring our manoeuvre traffic and have found that they can exploit traffic security weaknesses, such as use of P/L

We have our weaknesses, too!

weak argument

cryptanalytic success it does not involve any disclosure of methods. The line taken is "we see that you do this or that and we consider it on principle to be wrong" not "look how we can break your cyphers".

25. After the three parties have made one another aware of the elements of the problem they should constitute a tripartite advisory committee of communication security experts with terms of reference:

(i) to examine any weaknesses in national communication security systems of the three powers that may come to the knowledge of any one of them and may be regarded as affecting the interest of all;

(ii) to make recommendations for remedies;

(iii) to consider joint action in the common interest with regard to the security of other friendly powers.

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

26. Once the initial approach has been made there should be nothing to prevent any party from making further disclosures of any feature of his own security system on which he would like advice. Similarly there should be nothing to prevent any party who is in doubt about the security of another party's cryptosystem (but not able or perhaps not willing to prove that the system is insecure) from making a direct enquiry.

27. In considering the probable outcome of this approach and its effect on the [redacted] it should be borne in mind that the [redacted] ment is known to have set up, in 1951, an Interdepartmental Committee on [redacted] with a technical sub-committee, although each Ministry continues to produce its own cyphers and it is known that [redacted] and a man with considerable knowledge of cryptanalysis) is a member of one of these committees.(i) It must therefore be assumed either that the Committees are not properly informed of the current cypher practices of the various Ministries, or of the purposes for which certain cyphers are used or that (though informed) ~~they are~~ unable for one reason or another to make all the improvements that they would wish.

28. It will certainly not be difficult to convince the [redacted] representatives that they ought not to use the lower grade [redacted] cyphers and no harm would be done if we were to show them some examples. This is likely to come as a most unpleasant surprise to them for it is inconceivable that responsible [redacted] cryptographic experts can already know of the subjects for which the [redacted] that have

(i) Conversation between [redacted] and [redacted]

EO 3.3(h)(2)

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

no security value whatever.

29. When it comes to the higher grade systems it is however necessary to consider whether the [redacted] could be convinced of the insecurity of their systems without exposure of some more or less "sophisticated" techniques:

embarrassment due to inference info comes from either ① cryptanalysis or ② espionage

(i) [redacted] will have to describe the [redacted] practices which they consider unsound. That they know anything at all of these practices is of course in fact due to cryptanalysis, but they need not and should not describe the methods used to arrive at their information; it ought to be enough to describe the systems used as they find them, and to point out either that they are fundamentally insecure, or that they are being compromised by misuse.

Who?

(ii) The [redacted] already know enough of the weaknesses of the [redacted] to make it fairly easy to convince them that they are thoroughly insecure, without describing the techniques used in breaking. They also know that [redacted] can be broken.

(iii) The [redacted] machine is a pretty good cypher grossly misused by the [redacted] by repeated use of message settings through operator's carelessness or through use of an invariable "engineer's key", and by bad indicator systems. All these practices are so obviously wrong that the [redacted] could not want us to prove that we can take advantage of them.

(iv) Finally there is no need to show the [redacted] any of our actual decrypts. The cyphers in this group are obviously meant to carry secret correspondence.

III

MEASURES TO IMPROVE [redacted] CYPHERS

?

30. The probable upshot of the examination in committee of [redacted] [redacted] would be that the [redacted] experts are all too well aware of their deficiencies, that they have a long term programme for their improvement but that they are hampered by lack of material reources. The Committee will then have to proceed to consider ways and means of improvement; [redacted] should not decide at the Conference what they

(i) The [redacted] have already proposed an improvement of [redacted] (not we think adequate) and clearly know it is vulnerable. There is a suggestion in M. Charles Eyraud's "Precis de Cryptographie Moderne (1953)" that unmodified [redacted] at least is insecure.

propose to offer in the way of assistance and be agreed on pricrities but should endeavour in subsequent discussion with the [redacted] to apply their aid (which will certainly not amount to an immediate solution of the whole problem) wherever it best fits with [redacted] needs.

31. It is doubtful whether the C.C.M. machine proposed in the report of the 1951 conference should be offered now to the [redacted]

(i) The security of the machine, even with simplex settings, has been seriously challenged by [redacted] research since 1951[i]. It is not improbable that the [redacted] and indeed other members of NATO may have guessed this from the extraordinary changes in [redacted] regulations which have been promulgated in the past years and in the circumstances it would be wisest for [redacted] to forestall questions that might prove awkward by frankly admitting that they have come to fear that the machine is too easily compromised by operator's errors.

(ii) The 1951 proposals envisaged issue of 20 CCM immediately and a total of 80 eventually; it is probable that [redacted] would find it difficult to meet this programme today.

(iii) However if the [redacted] themselves would like a certain number of CCM, then these can be supplied within limits set by availability.

32. One-time pad, proposed in 1951, is an excellent solution, wherever practicable.

(i) The 1951 conference agreed that technical instruction in manufacture of random tables could be given to the [redacted] without disclosing cryptographic information[ii] and that this was an important and major requirement. It is still more important now that the [redacted] and others are showing signs of producing new and perhaps inferior methods of one time key generation. Rather than discuss these we would prefer to persuade the [redacted] that our own methods are well tried and sound, without however appearing to "instruct" them as if they were complete beginners in the are of making random key.

(ii) The allocation of one time pads is probably best organised by the [redacted] themselves. We should not, as was proposed by the U.K. in 1951, produce a ready made scheme of individual and multiple-address pads, which in our opinion

[i] The latest modification, "Lucifer", is a considerable improvement on the original machine, but even so CCM must be regarded as overdue for replacement.

[ii] Enclosure A para 33 1951 report.

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

would save them time and trouble. However suggestions from all parties could be considered in Committee.

(iii) The physical security provided by [redacted] methods of packaging OTP is likely to be of interest and it is recommended that it be described. (It is also possible that the [redacted] may wish to take into account the difficulties of physical security when considering any plan for multi-address pad systems).

(iv) There are undoubtedly ways of making the [redacted] much more nearly secure. These might well be considered subject to U.S. being able to provide a substantial number of [redacted] equipments and subject to the [redacted] finding them workable.

(v) The [redacted] is now regarded by [redacted] as very secure provided that the basic lug settings are chosen from limited lists which can be readily calculated on a large computing machine. If U.S. are able to make this machine available at an early date it would be very suitable for offer to [redacted] (or to other NATO powers) provided that a clear explanation were given of the reasons for using the limited list of basic lug settings. These reasons could be convincingly derived from first principles (need to ensure as even as possible a distribution of key values). Once again any attempt to dictate would be fatal, leading to suspicion of motives or wilful refusal to use the "good" list.

AFSAM-7. Where does this fit in?

33. It is hoped that enough has been said to dispose of the idea that the procedure advocated would lead to exposure of "sophisticated cryptanalytic techniques". (Appendix C to this paper contains examples taken from a recent [redacted] work on cryptanalysis with quotations from older works showing basic principles which are obviously commonplaces to any modern technician and which should suffice for a criticism of most if not all insecure European systems in use today).

?

IV

EXTENSION TO OTHER POWERS

34. It is proposed that other NATO powers, whose cyphers are held to be in need of improvement should in turn be invited to send representatives to the Tripartite Committee.

35. [redacted] would undoubtedly all have cypher experts capable of understanding and accepting the arguments used in assessing a cryptosystem. There is little fault to be found with their [redacted] and we have no knowledge of their [redacted] and could only obtain it by prolonged sigint study (likely to be most wasteful of effort) or by simply asking them for details. They should

[illegible] 1/[illegible]

our success not ultimate more effort would go further.

probably be left alone altogether or else regarded as potential givers of help.

[redacted]

(i) [redacted] has a one-time tape generator, believed secure.

(ii) [redacted] might perhaps undertake to educate [redacted] whose [redacted] is easily readable.

36. [redacted] is in similar case to [redacted] with much knowledge of crypto theory which is not applied in practice. Their [redacted] are largely insecure; nothing is known from Sigint of their [redacted] cyphers and it would be necessary to elicit information on these by direct questioning after we had indicated that we know the diplomatic systems to be insecure.

37. [redacted] too appears to be backward in crypt matters. It is known that the [redacted] are helping the [redacted] on Comint and it might be possible eventually for the [redacted] to approach them on Comsec, on which they are in very urgent need of advice.

gauge

38. It is difficult to guage the level of crypt knowledge in [redacted] they may all well have quite good cryptanalysts. Here again the only approach that can be tried with any hope of success is the educative one. If there is not already in these countries a crypt expert capable of appreciating the argument from first principles then they must begin by sending a man for a training course which should be based on the published literature.

V

CONCLUSION

not very good

[redacted]

39. Strange though it may seem, the security of a government's yphers is a most unreliable index of the skill of that government's ryptanalysts. If a nation uses bad cyphers the reason may be that they now no better, but it is much more likely to be that their policy kers fail to make use of the advice of their own technicians (which n some cases may be enough to take them most, if not all, of the way o real security) or else that they simply lack resources-material, ndustrial or financial-to carry out what they know to be necessary. If [redacted] come forward now, insisting on a critical examination of the situation (based on a realistic acknowledgement of certain facts about cryptography that are already pretty well known) and offering help from their own experience and material resources, they can guide their allies into use of cryptosystems that will stand up against the most advanced techniques known to [redacted] ~~and in doing so need~~

??

by or to whom?

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

DGC/3441

??

not disclose these techniques. If however they continue to turn a blind eye to the progress in cryptanalysis made all over Europe since 1939, and to refuse to talk about subjects that are in fact far less secret than they would like them to be, then they must expect to see European powers turn elsewhere for advice and assistance, and so to lose the opportunity to influence development in the right direction. Subsequently they may find that a situation has developed which they are unable to correct without making really damaging disclosures of advanced cryptanalysis in discussion, not only with officers of Allied Governments but also with commercial firms in neutral countries who manufacture equipment for sale to all comers. This danger is real, and if [redacted] wish to avoid such a situation they have no time to lose.

[redacted]

40. Finally, [redacted] must not expect the advice to be all one way, at least if the discussions are extended to [redacted] tions. They may well find that although their own cyphers are for the most part sound, yet nevertheless they are giving away in peacetime secret information, not obtainable by any other means, through excessive use of plain language and over simplification of signal procedure. Foreign Comint org nisations who have [redacted] may be able to help materially in assessing the extent of leakage arising in this way.

We know this only too well already

DGC/3441

Appendix 'A'

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

APPEN. A

I

CONTENT OF DIPLOMATIC TELEGRAMS

1. The [redacted] follow the rule that no NATO documents or accounts of NATO meetings may be passed in national cyphers fairly strictly. Only one instance is known to the contrary. Over the last two years they have become increasingly careful in the content of telegrams passed in their highly vulnerable medium grade cyphers, although their concern is to protect specifically [redacted] secrets rather than Allied secrets. In spite of this trend towards an improvement, however, cases still occur fairly frequently of serious compromises of Allied thought and intention in [redacted], sometimes in the medium grade cyphers. Examples are a report of March 1953 that [redacted] had promised an armoured division for the Middle East in war [redacted] and reports of January and February 1953 on [redacted] views on the European Defence Community [redacted] these last two in medium grade cypher). Apart from questions concerning [redacted] allies, the value of the information contained in the telegrams on [redacted] policy and on areas where the [redacted] are in a favourable position to obtain information are clearly of greater value to unfriendly powers than to [redacted] allies. The general assessment of [redacted] must therefore be that they still present a serious danger.

2. [redacted] commonly use their diplomatic cyphers for [redacted] questions. The [redacted] send long reports from [redacted] to [redacted] on discussions within SHAPE, slanted naturally towards [redacted] interests, but with a great deal of compromising detail. (For an example see [redacted] The cypher used for these reports is particularly vulnerable when the telegrams are long. The [redacted] are equally revealing. (See for example [redacted] giving plans for the development of the [redacted] and airfields up to and including 1955). [redacted] telegrams on the [redacted] give away less detail than the corresponding [redacted] telegrams, but can be most unfortunate. (See for example [redacted] showing that General Ridgeway's report in October to the Atlantic Council was passed by this means.) The [redacted] have shown some improvement over the past two years in their use of [redacted] subjects, but still make occasional revealing statements. (See for example the suggestion in [redacted] that of the western countries [redacted] were most inclined to be impressed by the recent Russian change of tactics). The cyphers of all these four countries are vulnerable, and it must be possible for the Russians from their telegrams to arrive at a clear appreciation of NATO plans and policies in Europe, and of the relationships of the allies to each other.

3. [redacted] cyphers are also vulnerable but are used with greater reticence. The worst example of a compromise is probably a [redacted]

DGC/3441

Appendix 'A'

II

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

CONTENT OF ARMED FORCES COMMUNICATIONS

4. The work being done on armed forces cyphers of NATO countries by the [redacted] is restricted almost entirely to [redacted] machine systems in [redacted] Both are vulnerable. Knowledge of the content of the messages would be of the very greatest value tactically to the Viet Minh forces and they would also yield considerable longer-term intelligence. The two systems are used for, among other things, daily situation reports, announcement of [redacted] plans, statements on allied co-operation with the [redacted] activities.

III

DEVELOPMENTS IN WAR

5. The above paragraphs are concerned with what is being given away by insecure cyphers of allied powers in present conditions. The value of similar information to an enemy in wartime would of course be much greater. The continued use by the [redacted] of insecure cyphers in active operations would, for example, be a very great danger not only to the [redacted] themselves but to their allies. Similar considerations apply to all other [redacted] in use by allies. That in wartime the cypher security of one ally must be the concern of all emerged quite clearly in the 1939-45 war, where we derived a great deal of intelligence on the [redacted] cyphers of all types.

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

DGC/3441

Appendix 'A'

Annexure 1

[redacted]

[redacted] are generally exploitable; they consist of badly-used [redacted] [redacted] There is little reference to NATO matters; the following examples are typical of information which does not represent a vital leakage, but which must be useful to the Russians:-

(a) Matters concerning the [redacted]

"Cockroft is to meet you in Brussels in order to discuss the exchange of [redacted] technicians gave me oral assurance of the fine functioning of [redacted]

(b) Details of arms shipments from America:-

[redacted]

(c) Off-shore purchases:-

[redacted]

ANX 1

2. The situation would be still more unfavourable in time of war, since such reports on arms deliveries in the present [redacted] [redacted] would give away details of Atlantic shipping movements.

DGC/3441

Appendix 'A'

Annexure 2

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

[redacted]

ANX 2

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

DGC/3441

Appendix 'A'

Annexure 2

[redacted]

5. Defence questions. The following [redacted] telegrams would be of value to Russia.

[redacted]

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

DGC/3441

Appendix 'A'

Annexure 2

[redacted]

In addition there is a considerable quantity of telegrams on the European Defence Community negotiations and on the Middle East Defence Organisation. The intelligence contained in them is not of vital significance to Russia, but it certainly provides useful background information. Some examples are:-

[redacted]

DGC/3444

Appendix 'A'

Annexure 2

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

6. Far East. The following telegrams would be of value to the Russians and their [redacted] allies:-

[redacted]

DGC/3441

Appendix 'A'

Annexure 2

(b) It has to be recognised that the [redacted] are less scrupulous when reporting comments by representatives of other countries, even though allied. See for example:-

[redacted]

comment (para 4(i) above) in FFDBF
" (para 4(c) ") "
" (para 6(d) ") "
" (para 6(e) ") "
" (para 4(h) ") "
" (para 3(b) ") "

(c) [redacted] are particularly cautious and limit themselves to comments on the press and on subjects of common knowledge. Care is evidently taken to include nothing of value.

(d) [redacted]

(e) [redacted]

(f) It must be remembered that the amount of [redacted] that has been read during the period under review was not been very great. It is a matter of speculation whether those [redacted] which we have not been able to exploit have in fact provided other instances of insecurity, and whether the Russians may have been able to exploit them.

9. Conclusion.

From the above analysis, of published [redacted] texts it emerges that the amount of vital information given away by the [redacted] to the Russians is small, but that a considerable quantity of useful background information is passed insecurely.

[redacted]

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

DGC/3441

Appendix 'A'

Annexure 3

[redacted] NON DIPLOMATIC SYSTEMS

A. [redacted]

1. As used by th[redacted] can provide the enemy with a very complete picture of the military situation, both tactical and strategic. The following are but a few typical examples of the kind of intelligence involved, the majority dated September 1952 to March 1953:-

(a) A daily sitrep gives a detailed picture both of the effect of [redacted] view of enemy dispositions, strength etc.

"According to documents contained in the brief case belonging to the [redacted]

[redacted]

(b) [redacted] and knowledge of enemy plans, often sent in ample time for the enemy to act upon the information.

"... to bring up to strength the radio teams of Tonkin which could be paradropped, and to place two of them in Cochin China. These elements will have to be ready for use in operations beginning on 1st November 1952."

[redacted]

[redacted]

ANX 3

(c) Information concerning French Allies.

[redacted]

DGC/3441

Appendix 'A'

Annexure 3

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

(d) Strategic supplies.

[redacted]

(e) Tactical planning.

[redacted]

2. In addition, there is much evidence of the results of [redacted] Sigint which must be of value to the enemy and also detrimental to any Allied co-operation with [redacted] in the Sigint field. For example:-

[redacted]

B. [redacted]

3. [redacted] appear to be used fairly indiscriminately in [redacted] and in some cases reports in the same series are passed on the same links using either machine. The type of information given away by the two systems is thus very similar. In the sample examined the [redacted] appears to pass fewer messages of a higher level nature than the [redacted]

4. The following are some typical extracts from [redacted] decrypts:-

(a) A cryptanalytic Status Report:-

[redacted]

[redacted]

DCC/3441

Appendix 'A'

Annexure 3

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

(b) Tactical sitreps:-

"Friendly losses were 3 killed and 6 wounded". [redacted]

(c) [redacted]

(d) Report on strategic information not to be released to the press:-

[redacted]

(e) Knowledge of enemy order of battle:-

[redacted]

(f) Training programme:-

[redacted]

C. Miscellaneous

[redacted]

6. The following types of traffic have been seen:-

[redacted]

[redacted]

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

DGC/3441

Appendix 'A'

Annexure 3

7. The only other traffic seen here, which appears to be an intelligence producer, is the joint attache system [redacted], passing economic type information, for example:-

[redacted]

[redacted]

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

DCC/3441

Appendix 'A'

Annexure 4.

[redacted]

ANX 4

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

DGC/3441

Appendix 'A'

Annexure 4

(c) [redacted]

(

(e)

DGC/3441

Appendix 'A'

Annexure 5

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

[redacted]

ANX 5

DGG/3441

Appendix 'A'

Annexure 5

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

(d) Orders and shipments.

[redacted]

DGC/3441

Appendix 'A'

Annexure 6

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

[redacted]

4. Some other examples:-

(a) Defence preparedness.

[redacted]

ANX 6

DGC/3441

Appendix 'A'

Annexure 6

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

[redacted]

(b) Airfield construction.

[redacted]

(c) Supply of armaments.

[redacted]

(d) Infrastructure.

[redacted]

(e) [redacted]

DGC/3441

Appendix 'A'

Annexure 7

ANX 7

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

TURKEY

[redacted]

[redacted]

DGC/3441

Appendix 'A'

Annexure 7

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

[redacted]

(b) Present strength

[redacted]

(c) Production

[redacted]

(d) Stockpiling

[redacted]

(e) Communications

[redacted]

(f) U.S. - Spanish negotiations

[redacted]

[redacted]

DGC/3441

Appendix 'A'

Annexure 7

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

[redacted]

(a) Details of submarine radars.

[redacted]

(b) NATO exercise

[redacted]

(c) Intelligence

[redacted]

DGC/3441

Appendix 'B'

EXAMPLES OF COMPROMISE OF CO-BELLIGERENTS BY CYPHER COMMUNICATIONS IN WORLD WAR II

A. Italians compromise Germans

1. In the Italian "Legations in the Balkan capitals .... their Military Attaches talked so freely to Rome of German military movements that the Germans eventually held up their telegrams". (G.C. & C.S. Diplomatic and Commercial Sigint, Vol. I, p.20)

2. As regards Special Intelligence concerning the German Army in the Mediterranean area in 1941, "the Italian partner was doing much to fill the gap until the end of 1941, when he introduced notable improvements in cypher security". (G.C. & C.S. Army and Air Force Sigint, Vol.I, p. 226)

3. Italian "main-line cyphers ... yielded all through 1941 a flow of information which threw light not only on Italian dispositions and intentions but on those of the Germans as well ... An example was a signal in 'Tellera' [cypher] giving the full tank strength returns of the two German armoured divisions in the Western desert, at a time when no information of the sort was available from any other source". (G.C. & C.S. Army and Air Force Sigint, Vol. IX, p. 115)

4. "'Z3', the cypher used by the Centauro Battle Group in Tunisia, for instance, gave on three occasions the complete German-Italian order of battle for a whole sector". (Ibid., p. 116)

5. "Falco", an Italian Air Force "supplementary high-grade system ... besides giving a good picture of Italian-German Air Force liaison in the Aegean, carried a good deal of traffic of operational importance and provided advance notice of intended German reconnaissances in Asia Minor, Cyprus and Egypt". (Ibid., pp. 231-232)

B. Reciprocal Compromise of Germans and Italians

6. Throughout the Western Desert and North African campaigns, Rommel was deprived of supplies and the Italians lost most of their merchant-fleet largely as a result of Allied reading of German army, air force and (from August 1942) Mediterranean Enigma traffic and of Italian Hagelin (from July 1941) and low-grade traffic. So full and detailed was the information concerning shipping, routes and cargoes that the Allies were able to concentrate their attack proportionately to the Axis need of individual commodities.
(For statistics and details see G.C. & C.S. Naval Sigint, Vol. IV, pp. 158-163. See also G.C. & C.S. Naval History, Vol. XX and G.C. & C.S. Air and Military History, Vol. IV.)

DGC/3441

Appendix 'B'

C. Japanese compromise Germans

7. Japanese Naval Attache Cypher

Admiral Abe, the extremely efficient Head of the Japanese Mission to Berlin, signalled home all the information - and, considering German caution vis-a-vis their ally, it was an astonishing amount - that he managed to extract from German authorities in a machine cypher, known to the Allies as JNA 20.
(G.C. & C.S. Naval Sigint, Vol. II, p. 164)

"'We are all most impressed', wrote Dr. R.V. Jones, A.D.I. (Science), Air Ministry, 'by the technical statements, which contain a wealth and accuracy of detail regarding German Radar surpassing any other Intelligence source during this war. Moreover, they give us a very good insight into German policy of a much more direct nature than we have hitherto attained by other methods'. The Admiral went on to contribute first-class, and often detailed, information on innumerable subjects of air an military interest, as well as naval, including the German anti-invasion preparations and intentions in Northern France".
(G.C. & C.S. Naval Sigint, Vol. IV, p. 206. A list follows of ten naval scientific inventions (weapons and processes), a description of which was first received from this source.)

8. Japanese Military Attache Cypher

"In February 1944, the Japanese Military Attache in Vichy sent a report to Tokyo, based upon statements by General von Runstedt's Chief of Staff, outlining German defensive strategy against the invasion".
(G.C. & C.S. Naval History, Vol. XIX, p. 147. Details follow)

9. For information on the development of German jet aircraft from both naval and military attache cyphers, see G.C. & C.S. Air and Military History Vol XI pp. 19 37, 54-56.

D. Free French compromise the Allies

10. "A captured enemy cryptanalyst who had worked at N.A.A. St.4 from 1941 until 1945 gave an account of the [Fighting French] systems which had been in use in Syria and West Africa during the period ... He said that in Syria two systems had been employed ... Both had been read in their entirety, and had given a full picture of the strength and organisation of the de Gaullist forces and political administration in the country, as well as useful details of British troop movements - the latter especially valuable since the British cyphers could not normally be read. The West African cyphers .... were more difficult than the Syrian systems, but were usually soluble at least in part".
(G.C. & C.S. Army and Air Force Sigint, Vol. XI, p. 32)

Appendix 'B'

11. "After the North African landings serious attempts were made to persuade the Fighting French to adopt systems of British or American devising for high level communications. Those attempts perhaps naturally, were not specially successful at first. The proffered systems were accepted, and employed to some extent, but the use of private cyphers - often very insecure ones - continued, particularly for messages which it was desired the Allies should not see, and which, of course, were for that very reason of most value to the enemy. By 1944, however, an all-round improvement ... had taken place". (Ibid., p. 33)

DGC/3441

Appendix 'C'

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

EXAMPLES TAKEN FROM THE LITERATURE OF CRYPTANALYSIS AND CRYPTOGRAPHY SHOWING BASIC PRINCIPLES WHICH ARE OBVIOUSLY COMMONPLACES TO ANY MODERN TECHNICIAN

APPEN. C

1. [redacted] has recently had an opportunity to examine a copy of "Precis de Cryptographie Moderne" by Charles Eyraud. (Paris Editions Raoul Tari, 10 Rue de Buci, Paris VI^{e} 1953). This work is not for sale to the general public, but at the same time it carries no mark of security grading. The preface acknowledges help received by the author from Col. Black; the latter however has stated that he has had the book carefully "purged" of anything that might be prejudical to the work of his department.

2. It follows that the opinions expressed in this book do not necessarily represent the level of technical knowledge of the best French experts, e.g. it would be wrong to judge French knowledge of drum machines from the following curious passage relating to the German Enigma (which is badly and innacurately described):

Cover & Deception?

> "Thus one sees that the supplementary plugboard is a very important security factor. But even without it we cannot see how the drum wiring could be recovered. One may therefore state that this machine is practically indecypherable."

3. When, however, perfectly sound statements are made about the basic principles of cryptography one may assume that these are regarded as commonplaces.

4. The following extracts give examples of such statements, many of which are highly relevant to present French practices. It is noteworthy that many of these contain quotations from older works.

(On Cypher Machines in general)

(i) "There is no doubt that length (of key stream) on the one hand, and a large number of alphabets on the other, and finally the complexity of cyclic mechanisms, (including factors of irregularity which make reconstruction more difficult) are principal elements for appreciation of the cryptographic value of a machine. But they are not the only ones; one would be very wrong to believe that they constitute a formal and absolute indication.

Any machine has to be used properly. It must also be adapted to its use. "Some excellent razors are most dangerous in the hands of a monkey" (says Givierge) "and some delicate revolution counters would work badly on the wheel of a turf-barrow."

DCC/3441

Appendix 'C'

"The choice of agreed keys" according to General Sacco "must not be left to the initiative of cypher operators but must be made in a central office". Often in fact, if a change of the outer key does not affect the set up of the machine or the key series but only the starting point on the latter one may have re-use of a "portion of the key series already used for another message and in consequence long repeats which reveal the coincidence and help the cryptanalysis."

Part II Para 115

(ii) In assessing a machine, account should be taken of the fact that its permanent characteristics cannot remain secret, and also of all possible accidents.

IBID

(On the T-52 Machine)

(iii) "We have seen that for on-line teletype cyphers 120 single keys obtained by permutation of the five impulses are less efficacious than 32 keys obtained by change of polarity. This is enough to show that the crude number of single keys used is only a first indication."

IBID

(iv) Givierge has spoken of "malpractices that theory cannot predict though their existence is attested by experience" and more recently Sacco has added that "cypher operators do enough to help the enemy."

IBID Part III Para 36

(On additive systems)

(v) "Two cryptograms with the same recypher key can in theory be decrypted" "..... in practice it is necessary to have at least a third text".

IBID Part III Para 30

(On plain codes)

(vi) "In any case, as General Sacco says, secret codes are only secure on condition that they are not and never have been used without **recypherment**, the latter being very frequently changed."

IBID Part III Para 30

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

DGC/3441

20th May, 1953

Copy No.:...12.....

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

SECURITY OF THE [redacted] OF THE NATO POWERS

INTRODUCTION

[redacted]

The U.K. views are summarised in the following paragraphs:-

[redacted]

Evidence available from U.S.-U.K. [redacted] is sufficient, in the U K. view, to show that the following require remedial action.

[redacted]

[redacted]

The U.K. view is that the problem is one for discussion among communication security officers, and that it is essential for U.K. and U.S.

[redacted]

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

DGC/3441

[redacted]

[redacted]

DGC/344

I

SCOPE OF THE PROBLEM

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

(a) [redacted]

1. It was agreed at the U.K./U.S. Conference of May 1951 that it [redacted]

[redacted]

(b) [redacted]

4. The U.K./U.S. Conference of May 1951 considered and rejected [redacted]

"(i) [redacted]

(ii)

5. Although considerable progress has been made since 1951 in the [redacted]

(i) [redacted]

(ii)

6. The conclusion is that it is dangerous to leave the [redacted] Forces cyphers in their present condition and that they should be included in any future approach to the French; with the right sort of approach there should be no need for disclosure of "sophisticated techniques".

(c) [redacted]

7. The general question of improvement of the [redacted] of the other NATO powers has never been discussed officially between U.K. and U.S.

(i) The U.S. view on this subject in 1951 was however indicated by the following statement made by an ad hoc committee of U.S.C.I.B.

[redacted]

[redacted]

(ii) It was ultimately agreed that the U.S. Government should make

[redacted]

[redacted]

(ii)Report of U.S.C.I.B. ad hoc Committee on [redacted] Security, September, 1951.

(iii) [redacted]

8. The U.K. view is "shock tactics" of this kind are unlikely to be effective especially when they are accompanied by a "cover story" which is unlikely to be believed; the only way to achieve improvement in security habits is by educative action and by influence of the "public opinion" (if such a term may properly be used of a very secret subject) of other powers' Comsec officers.

9. But the dictum of the U.S.C.I.B. ad hoc Committee referred to in para 7 above has in the U.K. view another serious weakness in that it is based on the assumption that it is possible in matters of cypher security to "have it both ways". This assumption has appeared at various times in discussion in two different forms:

(i) that it is possible to devise cyphers that are just good enough to defeat the Russians but contain weaknesses that can be exploited by U.K./U.S.; we cannot know anything of the level of competence of U.S.S.R. cryptanalysts.

(ii) that it is sufficient to limit improvement of security to specified cryptochannels or to telegrams on specified subjects. This will not do; it is not possible to forecast in advance which cryptochannels are going to carry important messages and it is not enough to insist on use of NATO cyphers when documents are [redacted] without also taking steps to protect the security of NATO fringe traffic or national comment on NATO discussions which may legitimately be sent in national cyphers.

(d) Armed Force Cyphers of the other NATO Powers

10. Little is known, from Sigint sources, of the armed forces cyphers of any European power except [redacted] and if as seems probable they are no better than the diplomatic cyphers they would be, in varying degrees, dangerous to the security of any forces operating with them in war.

(e) Cypher machine development in Europe

11. It is known that new cypher machines are being developed by several NATO governments and by commercial firms operating in neutral countries.

(i) The [redacted] have designed cypher machines which they intend to use for their armed forces; these machines embody some fiarly advanced techniques but from information at present available appear to be most insecure.(1)

(1) See memorandum from Italian Military Mission in Washington to Secretariat of the Standing Group, No. 0927/SRP ~~of 30.4~~.53,

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

(ii) [redacted]

(iii) The [redacted] in conjunction with a Swiss firm, is producing a wide range of new cypher machines which will undoubtedly be much better than the same firm's pre-war models, but may still be not secure against modern cryptanalytic methods.

12. This list is probably not exhaustive, and these developments merit close attention from U.K. and U.S. While it is entirley possible that European powers may work out their own salvation, with or without the aid of commercial firms it is to be feared that they may only arrive [redacted] of current U.K./U.S. thought on cypher machine design. It would be therefore better to approach these European powers before their own development has gone too far, and persuade then to adopt well tried U.K./U.S. methods.

(f) Decisions to be taken at the Conference

(A) Countries to be covered

[redacted]

(B) Timing of action with relation to physical security

14. The 1951 Conference agreed a limited programme for an approach [redacted] expressed themselves satisfied that such improvement has gone far enough.

15 While it is agreed that we ought to adjust our methods to take account of differing physical security conditions in various countries it may be said

(i) that physical leakages will seldom if ever be so gross as to provide a source of intelligence as rapid, complete, reliable and (above all) authentic as that derived from a major breakdown in communication security; conditions need to be literally hopeless before one can say that there is no point in improving cypher security;

(1) Conversation between [redacted] February 1953.

EO 3.3(h)(2)

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

(ii) One should however not delay initiating action on cypher security pending expected improvements in physical security, because neither can be put right overnight.

16. The U.K. recommendation is therefore that there is no case for any further delay in approaching the [redacted] and that physical security of other nations might be considered as a valid reason for taking no action at all, or for taking modified action but not for delaying action.

II

THE APPROACH TO THE [redacted]

17. Having settled the scope of action intened the Conference should in the U.K. view consider an approach to the [redacted] Government with a view to first improving their communications security and then inviting them to associate themselves with any scheme that may have been agreed between U.K. and U.S. for approaches to other NATO nations.

18. It is recommended that a single approach be made to the [redacted] covering all cyphers of all services in respect of which the conference has decided that action must be taken.

19. Previous projects for approach to the [redacted] Government on the delicate subject of the security of their national cyphers have been based on the assumption that this insecurity is due to ignorance of the art of cryptography which cannot be removed without exposure of "sophisticated" cryptanalytic techniques. Yet after all the basic principles of cryptography are few, simple and well known to all cypher experts including the [redacted] and do not constitute the "secret" upon which the success of cryptanalysis depends. The "secrets" of cryptanalysis are rather these:

(i) that situations arise in the use of cyphers which would instantly be condemned as insecure by any one instructed in cryptography;

(ii) that other situations arise which an instructed person would admit to offer at least a theoretical risk of insecurity, but which require "sophisticated techniques" to exploit them, and that these techniques have been devised.

20. The only way in which improvement in [redacted] can be eventually obtained is by cooperation on the technical level between [redacted] [redacted] communication security officers.

21. The object of the first approach therefore would ~~be to~~ bring about a frank exchange of information that would serve as a basis for

subsequent discussion among responsible communication security officers. One of the points that the Conference must decide is whether this initial exchange should be made:

(i) at a tripartite meeting;

(ii) at separate bipartite meetings, [redacted]

(iii) at a single bipartite meeting where either U.K. or U.S. [redacted]

22. The tripartite arrangement would be the best, apart from the fact that it would be impossible to conceal the fact that U.K. and [redacted] undoubtedly be assumed. It is therefore recommended that the meeting be tripartite.

23. The exchange can be initiated in two ways only:

(i) by inviting each party to describe its own communication security methods, which would then be discussed on general cryptographic grounds by the other two.

(ii) [redacted]

24. The second approach is recommended, as being more sure of its effect.

(i) Initially at least it may be somewhat embarrassing but it will have less long term disadvantages in that it does not commit anybody to disclosure of details of their own systems which they consider irrelevant or do not wish to mention.

(ii) Although this approach implies a tacit admission of

(i) This is something more than a polite fiction. We already know that the [redacted]h have been monitoring our manoeuvre traffic and have found that they can exploit traffic security weaknesses, such as use of P/L.

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

cryptanalytic success it does not involve any disclosure of methods. The line t aken is "we see that you do this or that and we consider it on principle to be wrong" not "look how we can break your cyphers".

25. After the three parties have made one another aware of the elements of the problem they should constitute a tripartite advisory committee of communication security experts with terms of reference:

(i) to examine any weaknesses in national communication security systems of the three powers that may come to the knowledge of any one of them and may be regarded as affecting the interest of all;

(ii) to make recommendations for remedies;

(iii) to consider joint action in the common interest with regard to the security of other friendly powers.

[redacted]

(i) Conversation between [redacted]

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

no security value whatever.

29. When it comes to the higher grade systems it is however necessary to consider whether the [redacted] could be convinced of the insecurity of their systems without exposure of some more or less "sophisticated" techniques:

(i) [redacted]

(ii)

(iii)

(iv)

III

MEASURES TO IMPROVE [redacted] CYPHERS

[redacted] improvement; U.K. and U.S. should not decide at the Conference what they

[redacted]

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

DGC/3441

propose to offer in the way of assistance and be agreed on priorities but should endeavour in subsequent discussion with the [redacted] to apply their aid (which will certainly not amount to an immediate solution of the whole problem) wherever it best fits with French needs.

31. It is doubtful whether the C.C.M. machine proposed in the report of the 1951 conference should be offered now to the [redacted].

(i) [redacted]

(ii) The 1951 proposals envisaged issue of 20 CCM immediately and a total of 80 eventually; it is probable that U.K./U.S. would find it difficult to meet this programme today.

(iii) However if the [redacted] would like a certain number of CCM, then these can be supplied within limits set by availability.

32. One-time pad, proposed in 1951, is an excellent solution, wherever practicable.

(i) The 1951 conference agreed that technical instruction in manufacture of random tables could be given to the [redacted] without disclosing cryptographic information(ii) and that this was an important and major requirement. It is still more important now that the [redacted] and others are showing signs of producing new and perhaps inferior methods of one time key generation. Rather than discuss these we would prefer to persuade the [redacted] that our own methods are well tried and sound, without however appearing to "instruct" them as if they were complete beginners in the are of making random key.

(ii) The allocation of one time pads is probably best organised by the [redacted] themselves. We should not, as was proposed by the U.K. in 1951, produce a ready made scheme of individual and multiple-address pads, which in our opinion

(i) The latest modification, [redacted], is a considerable improvement on the original machine, but even so CCM must be regarded as overdue for replacement.

(ii) Enclosure A para 33 1951 report.

would save them time and trouble. However suggestions from all parties could be considered in Committee.

(iii) The physical security provided by [redacted] methods of packaging OTP is likely to be of interest and it is recommended that it be described. (It is also possible that the [redacted] may wish to take into account the difficulties of physical security when considering any plan for multi-address pad systems).

(iv) There are undoubtedly ways of making the M209 much more nearly secure. These might well be considered subject to U.S. being able to provide a substantial number of M209 equipments and subject to the [redacted] finding them workable.

(v) The [redacted] is now regarded by [redacted] as very secure provided that the basic lug settings are chosen from limited lists which can be readily calculated on a large computing machine. - If U.S. are able to make this machine available at an early date it would be very suitable for offer to [redacted] (or to other NATO powers) provided that a clear explanation were given of the reasons for using the limited list of basic lug settings. These reasons could be convincingly derived from first principles (need to ensure as even as possible a distribution of key values). Once again any attempt to dictate would be fatal, leading to suspicion of motives or wilful refusal to use the "good" list.

33. It is hoped that enough has been said to dispose of the idea that the procedure advocated would lead to exposure of "sophisticated cryptanalytic techniques". (Appendix C to this paper contains examples taken from a recent [redacted] work on cryptanalysis with quotations from older works showing basic principles which are obviously commonplaces to any modern technician and which should suffice for a criticism of most if not all insecure European systems in use today).

IV

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

EXTENSION TO OTHER POWERS

34. It is proposed that other NATO powers, whose cyphers are held to be in need of improvement should in turn be invited to send representatives to the Tripartite Committee.

35. [redacted] would undoubtedly all have cypher experts capable of understanding and accepting the arguments used in assessing a cryptosystem. There is little fault to be found with their [redacted] and we have no knowledge of their [redacted] and could only obtain it by prolonged sigint study (likely to be most wasteful of effort) or by simply asking them for details. They should

probably be left alone altogether or else regarded as potential givers of help.

(i) [redacted] has a one-time tape generator, believed secure.

(ii) [redacted]

[redacted]

37. [redacted] too appears to be backward in crypt matters. It is known that the [redacted] are helping the [redacted] on Comint and it might be possible eventually for the [redacted] to approach them on Comsec, on which they are in very urgent need of advice.

38. It is difficult to guage the level of crypt knowledge in [redacted]; they may all well have quite good cryptanalysts. Here again the only approach that can be tried with any hope of success is the educative one. If there is not already in these countries a crypt expert capable of appreciating the argument from first principles then they must begin by sending a man for a training course which should be based on the published literature.

V

CONCLUSION

39. Strange though it may seem, the security of a government's cyphers is a most unreliable index of the skill of that government's cryptanalysts. If a nation uses bad cyphers the reason may be that they know no better, but it is much more likely to be that their policy makers fail to make use of the advice of their own technicians (which in some cases may be enough to take them most, if not all, of the way to real security) or else that they simply lack resources-material, industrial or financial-to carry out what they know to be necessary. If [redacted] come forward now, insisting on a critical examination of the situation (based on a realistic acknowledgement of certain facts about cryptography that are already pretty well known) and offering help from their own experience and material resources, they can guide their allies into use of cryptosystems that will stand up against the most advanced techniques known to N.S.A. and G.C.H.Q., and in doing so need

not disclose these techniques. If however they continue to turn a blind eye to the progress in cryptanalysis made all over Europe since 1939, and to refuse to talk about subjects that are in fact far less secret than they would like them to be, then they must expect to see European powers turn elsewhere for advice and assistance, and so to lose the opportunity to influence development in the right direction. Subsequently they may find that a situation has developed which they are unable to correct without making really damaging disclosures of advanced cryptanalysis in discussion, not only with officers of Allied Governments but also with commercial firms in neutral countries who manufacture equipment for sale to all comers. This danger is real, and if U.K. and U.S. wish to avoid such a situation they have no time to lose.

40. Finally, U.K. and U.S. must not expect the advice to be all one way, at least if the discussions are extended to Armed Forces communications. They may well find that although their own cyphers are for the most part sound, yet nevertheless they are giving away in peacetime secret information, not obtainable by any other means, through excessive use of plain language and over simplification of signal procedure. Foreign Comint organisations who have intercepted U.K., U.S. traffic may be able to help materially in assessing the extent of leakage arising in this way.

DGC/3441

Appendix 'A'

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

I

[redacted]

DGO/3441

Appendix 'A'

II

CONTENT OF ARMED FORCES COMMUNICATIONS

4. The work being done on armed forces cyphers of NATO countries by the U.K. and the U.S. is restricted almost entirely to [redacted]. Knowledge of the content of the messages would be of the very greatest value tactically to the Viet Minh forces and they would also yield considerable longer-term intelligence. The two systems are used for, among other things, daily [redacted]

III

DEVELOPMENTS IN WAR

5. The above paragraphs are concerned with what is being given away by insecure cyphers of allied powers in present conditions. The value of similar information to an enemy in wartime would of course be much greater. The continued use by the [redacted] of insecure cyphers in active operations would, for example, be a very great danger not only to the French themselves but to their allies. Similar considerations apply to all other armed forces and diplomatic cyphers in use by allies. That in wartime the cypher security of one ally must be the concern of all emerged quite clearly in the 1939-45 war, where we derived a great deal of intelligence on the [redacted] cyphers of all types.

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

DGC/3441

Appendix 'A'

Annexure 1

[redacted]

(a) Matters concerning the Atomic Energy Commission:-

[redacted]

(b) Details of arms shipments from America:-

[redacted]

(c) Off-shore purchases:-

[redacted]

2. The situation would be still more unfavourable in time of war, since such reports on arms deliveries in the present [redacted] [redacted] would give away details of [redacted] movements.

DGC/3441

Appendix 'A'

Annexure 2

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

[redacted]

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

DGC/3441

Appendix 'A'

Annexure 2

[redacted]

DGC/3441

Appendix 'A'

Annexure 2

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

(c) [redacted]

In addition there is a considerable quantity of telegrams on the [redacted] and on the [redacted] Organisation. The intelligence contained in them is not of vital significance to Russia, but it certainly provides useful background information. Some examples are:-

(a)

(b)

(c)

(d)

((e)

(f)

(g)

(h)

[redacted]

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

DGC/344A

Appendix 'A'

Annexure 2

[redacted]

7. Other topics.

[redacted]

8. Some general remarks.

(a) [redacted]

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

DGC/3441

Appendix 'A'

Annexure 2

[redacted]

9. Conclusion.

From the above analysis, of published [redacted] texts it emerges that the amount of vital information given away by the [redacted] to the Russians is small, but that a considerable quantity of useful background information is passed insecurely.

DGC/3441

Appendix 'A'

Annexure 3

FRENCH NON DIPLOMATIC SYSTEMS

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

A. [redacted]

1. As used by the [redacted] can provide the enemy with a very complete picture of the military situation, both tactical and strategic. The following are but a few typical examples of the kind of intelligence involved, the majority dated September 1952 to March 1953:-

[redacted]

(c) Information concerning [redacted] Allies.

[redacted]

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

DGC/3441

Appendix 'A'

Annexure 3

(d) Strategic supplies.

[redacted]

(e) Tactical planning.

[redacted]

2. In addition, there is much evidence of the results of [redacted] [redacted] which must be of value to the enemy and also detrimental to any Allied co-operation with [redacted] For example:-

[redacted]

B. [redacted]

3. The [redacted] appear to be used fairly indiscriminately in Indo-China, and in some cases reports in the same series are passed on the same links using either machine. The type of information given away by the two systems is thus very similar. In the sample examined the [redacted] appears to pass fewer messages of a higher level nature than the [redacted]

4. The following are some typical extracts from [redacted]

(a) A cryptanalytic Status Report:-

[redacted]

DGC/3441

Appendix 'A'

Annexure 3

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

(b) Tactical sitreps:-

[redacted]

[redacted]

(d) Report on strategic information not to be released to the press:-

[redacted]

(e) Knowledge of enemy order of battle:-

[redacted]

(f) Training programme:-

[redacted]

C. Miscellaneous

[redacted]

6. The following types of traffic have been seen:-

[redacted]

DGC/3441

Appendix 'A'

Annexure 3

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

7. The only other traffic seen here, which appears to be an [redacted]

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

DGC/3441

Appendix 'A'

Annexure 4

[redacted]

[redacted]

[redacted]

4. The following are some examples of the type of information still passing:-

[redacted]

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

DGC/3441

Appendix 'A'

Annexure 4

(c) [redacted]

(Greek-Yugoslav relations.

[redacted]

(e) MEDO.

[redacted]

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

DGC/34 41

Appendix 'A'

Annexure 5

[redacted]

The main [redacted] which as used by the [redacted] is quite insecure and could be read by any organisation possessing rapid analytical machinery. Other systems, usually code with additive, are occasionally read, but do not normally concern major political subjects. There is also a [redacted] believed to be [redacted] which is not at present readable.

2. The [redacted] and more particularly the [redacted] links pass a considerable number of reports on NATO matters, and the [redacted] has made a practice of reporting on [redacted] although in less detail than the [redacted] [redacted] There is some evidence that they are aware of their cypher responsibilities in this matter. For example, [redacted] gives a general report on an American statement made at a meeting of the Atlantic Council, and concludes by saying that the text of the statement would be sent in Typex.

3. Nevertheless, reading of this traffic must give the Russians a fairly comprehensive picture of general NATO planning and equipment. For example:-

(a) Reports on NATO meetings

[redacted]

(b) German attitude to EDC

[redacted]

(c) Equipment policy

[redacted]

DGC/3441

Appendix 'A'

Annexure 5

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

(d) Orders and shipments.

[redacted]

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

DGC/3441

Appendix 'A'

Annexure 6

PORTUGAL

[redacted]

4. Some other examples:-

(a) Defence preparedness.

[redacted]

DGC/3441

Appendix 'A'

Annexure 6

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

[redacted]

(b) Airfield construction.

[redacted]

(c) Supply of armaments.

[redacted]

(d) Infrastructure.

[redacted]

(e) German participation.

[redacted]

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

DGC/3441

Appendix 'A'

Annexure 7

[redacted]

[redacted] is particularly bad. The main [redacted] even the [redacted] introduced in October 1952 for NATO matters can be fully solved on messages of more than 500 groups, and a high proportion of messages are of considerable length. The military [redacted] badly used and quite easily readable, [redacted]i analytical machinery. Nothing is known of [redacted] but it must be assumed that they are quite insecure and may be giving away considerable detailed information of tactical and strategic value.

2. [redacted] yields a wealth of information on NATO planning, strategy, equipment, etc., which must be of very high value to the Russians. The following examples are typical of the intelligence provided:-

(a) The [redacted] contribution in case of war.

[redacted]

DGC/3441

Appendix 'A'

Annexure 7

[redacted]

(b) Present strength

[redacted]

(c) Production

[redacted]

(d) Stockpiling

[redacted]

(e) Communications

[redacted]

(f) [redacted] negotiations

[redacted]

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

-3

DGC/3441

Appendix 'A'

Annexure 7

[redacted]

(a) Details of submarine radars.

[redacted]

(b) NATO exercise

[redacted]

(c) Intelligence

[redacted]

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

DGC/3441

Appendix 'B'

EXAMPLES OF COMPROMISE OF CO-BELLIGERENTS BY CYPHER COMMUNICATIONS IN WORLD WAR II

A. [redacted]

B. Reciprocal Compromise of [redacted]

[redacted]

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

DGC/3441

Appendix 'B'

C. [redacted]

D.

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

[redacted]

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

DGC/3441

Appendix 'C'

EXAMPLES TAKEN FROM THE LITERATURE OF CRYPTANALYSIS AND CRYPTOGRAPHY SHOWING BASIC PRINCIPLES WHICH ARE OBVIOUSLY COMMONPLACES TO ANY MODERN TECHNICIAN

1. [redacted] has recently had an opportunity to examine a copy of "Precis de Cryptographie Moderne" by Charles Eyraud. (Paris Editions Raoul Tari, 10 Rue de Buci, Paris VI^{e} 1953). This work is not for sale to the general public, but at the same time it carries no mark of security grading. The preface acknowledges help received by the author from Col. Black; the latter however has stated that he has had the book carefully "purged" of anything that might be prejudical to the work of his department.

2. It follows that the opinions expressed in this book do not necessarily represent the level of technical knowledge of the best French experts, e.g. it would be wrong to judge French knowledge of drum machines from the following curious passage relating to the German Enigma (which is badly and innacurately described):

> "Thus one sees that the supplementary plugboard is a very important security factor. But even without it we cannot see how the drum wiring could be recovered. One may therefore state that this machine is practically indecypherable."

3. When, however, perfectly sound statements are made about the basic principles of cryptography one may assume that these are regarded as commonplaces.

4. The following extracts give examples of such statements, many of which are highly relevant to present French practices. It is noteworthy that many of these contain quotations from older works.

(On Cypher Machines in general)

(i) "There is no doubt that length (of key stream) on the one hand, and a large number of alphabets on the other, and finally the complexity of cyclic mechanisms, (including factors of irregularity which make reconstruction more difficult) are principal elements for appreciation of the cryptographic value of a machine. But they are not the only ones; one would be very wrong to believe that they constitute a formal and absolute indication.

Any machine has to be used properly. It must also be adapted to its use. "Some excellent razors are most dangerous in the hands of a monkey" (says Givierge) "and some delicate revolution counters would work badly on the wheel of a turf-barrow."

"The choice of agreed keys" according to General Sacco "must not be left to the initiative of cypher operators but must be made in a central office". Often in fact, if a change of the outer key does not affect the set up of the machine or the key series but only the starting point on the latter one may have re-use of a "portion of the key series already used for another message and in consequence long repeats which reveal the coincidence and help the cryptanalysis."

Part II Para 115

(ii) In assessing a machine, account should be taken of the fact that its permanent characteristics cannot remain secret, and also of all possible accidents.

IBID

(<u>On the T-52 Machine</u>)

(iii) "We have seen that for on-line teletype cyphers 120 single keys obtained by permutation of the five impulses are less efficacious than 32 keys obtained by change of polarity. This is enough to show that the crude number of single keys used is only a first indication."

IBID

(iv) Givierge has spoken of "malpractices that theory cannot predict though their existence is attested by experience" and more recently Sacco has added that "cypher operators do enough to help the enemy."

IBID Part III Para 36

(<u>On additive systems</u>)

(v) "Two cryptograms with the same recypher key can in theory be decrypted" "..... in practice it is necessary to have at least a third text".

IBID Part III Para 30

(<u>On plain codes</u>)

(vi) "In any case, as General Sacco says, secret codes are only secure on condition that they are not and never have been used without **recypherment**, the latter being very frequently changed."

IBID Part III Para 30