5 FCP 46

~~TOP SECRET~~

TOP SECRET

Appendix ____ to British - U. S. C. I. Agreement

Regulations for the coordination of British - U. S. cryptanalysis, traffic analysis, and associated techniques

OUTLINE

I The Responsibility for Traffic Analysis

II The Means of Allocation of Crytpanalytic Tasks

- A. Establishment and Functions of the Allocation Committee
- B. Principles to be Followed in the Allocation of Cryptanalytic Tasks
- C. Assistance by Other Party
- D. Activity of Other Party
- E. Termination of Allocation
- F. Protection of National Interests

I The Responsibility for Traffic Analysis

II The Allocation of Cryptanalytic Tasks

III Subject Matter of Exchange

- A. Intelligence
- B. Technical Products
- C. Methods and Techniques
- D. Personnel

IV Means and Manner of Making Reports

- A. Methods of Transmittal
- B. Time of Making Reports
- C. Reports of Liaison Officers
- D. Forms of Reports
- D. Standardization of Terminology
- E. Standardization of Reports

V. Definitions

- Communication
- Traffic Analysis
- Traffic Intelligence
- Cryptanalysis
- Cryptanalytic Achievement

~~TOP SECRET~~

TOP SECRET

I The Responsibility for Traffic Analysis.

Traffic analysis will not be allocated as such, but the party which performs the interception shall be primarily responsible for the appertaining traffic analysis, with the other party rendering such assistance as may be practicable.

II The Means of Allocation of Cryptanalytic Tasks.

A. Establishment and Functions of the Allocation Committee.

1. STANCIB and SIGINT will establish and provide for the organization of a permanent committee for the allocation of cryptanalytic tasks.
2. The committee shall have the responsibility of making an initial allocation of cryptanalytic tasks and the continuing responsibility of making new allocations and re-allocations to the end that there is at all times a complete coverage of the work to be done.
3. In making all allocations, the committee shall adhere to the principles set forth in Paragraph II B hereof.
4. Each party shall supply the committee with all information which it may consider that it needs.
5. Action of the committee shall be only by unanimous consent.

B. Principles to be Followed in the Allocation of Cryptanalytic Tasks.

? 1. All systems in which a party has a primary national interest shall be allocated to that party. Any system, however, in which both parties claim a primary national interest, shall be allocated to both parties.
2. All systems not allocated to one or both of the parties under the preceding paragraph shall be considered to fall into one of the following two categories:
   a. Those from which intelligence is wanted because of the known or suspected value of the information;
   b. Those of known or expected low intelligence value.
3. Each system in category 2a shall be allocated on the basis of the following principles progressively considered:
   a. Available capacity in terms of personnel and other facilities for handling the task. (Since the primary purpose of allocation is to produce maximum intelligence, the first consideration in the allocation of a task is always to place the task where it can be done best. Each party accordingly will be given tasks appropriate to the facilities and talents available and, insofar as possible, in sufficient volume to utilize completely its full potentialities).
   b. If personnel and other facilities are equally available, systems related cryptographically and systems whose texts will permit cross-working shall normally be assigned to the same party. (e.g., assuming that each party has facilities available for more work, that a system with "Y" cryptographic characteristics is being considered for allocation,

I The Responsibility for Traffic Analysis.

1. Each party separately is responsible for all traffic analysis tasks.
2. However because of the close association of traffic analysis with the intercept stations, a primary responsibility for traffic analysis of a given area will fall on that party controlling the intercept.

II Allocation of Cryptanalytic Tasks.

1. Each party separately is responsible for all cryptanalytic tasks.
2. In the event that one party through lack of equipment or personnel is unable to perform certain of its cryptanalytic tasks, these tasks by mutual agreement of the operating agencies may be allocated to one of the parties.
3. Should a party to whom a task has been so allocated determine to discontinue its efforts, prompt notification will be made to the other party.
4. Each agency will endeavor to comply with requests for the occasional use of special equipment applicable to traffic analysis or cryptanalysis.

and that Party "A", through prior allocation, has developed facilities for attacking "Y" type problems, then the new system of "Y" type should be allocated to Party "A"; systems which have their most useful [redacted]n systems allocated to Party "A" should likewise be allocated to Party "A").

c. If the consideration of available personnel and facilities and cryptographic characteristics does not determine the allocation, then the relationships of the textual content to (i) primary assignment and (ii) primary interest shall control.

4. Each system in category 2b shall be allocated on the basis of the following principles progressively considered:

a. A system shall be allocated to the party which has the greater need for it for training purposes;

b. If the needs of the parties for training purposes are approximately equal, a system shall be allocated on the basis of relation in general interest to previously allocated systems (e.g., if Country X is an originator in several fields and its traffic is considered to be unimportant, all of its systems might be allocated to Party "A" on the ground that Country Y, a near neighbor of Country X, had previously been allocated to Party "A").

c. Any remaining systems shall be allocated in accordance with the judgment of the allocation committee.

OGA
EO 1.4.(c)
EO 1.4.(d)

5. No allocation shall be made as to the following foreign countries, it being the intention that no collaboration or exchange will take place as to them:

[redacted]

C. Assistance by Other Party.

Although a particular system has been allocated to one party, it may develop that the other party has a special interest from the technical point of view in a problem presented by the work on that system or has available facilities or techniques, including possibly a withheld technique, which might be useful in making the attack. In such case, the party to which the system has been allocated may request the assistance of the other party, or the other party may offer its assistance. As a general rule, such assistance will be given or accepted, as the case may be.

D. Activity of Other Party.

For the purpose of keeping in touch with all problems, each party is priveleged to engage in research and decryption in relation to systems allocated to the other party. In the event of a shortage of facilities, however, it is the obligation of a party to handle first the work on the systems allocated to it and to subordinate its activities on the systems allocated to the other party.

TOP SECRET

E. Termination of Allocation.

If a party lacks the interest or facilities to exert proper effort to perform its obligation as to a system allocated to it, it shall so notify the allocation committee, whereupon the party's responsibility ends. The allocation committee shall then offer the system to the other party, which may accept or reject, as it sees fit.

F. Protection of National Interests.

In order that each party may protect its national interests as it sees them, each party shall always be free to work on any communication system of any foreign country.

~~TOP SECRET~~

III Subject Matter of Exchange.

A. Intelligence

1. As to each foreign country, except those excluded from collaboration and exchange, either party, which recovers any intelligence by cryptanalysis or traffic analysis, will deliver all intelligence so recovered to the other party. This will always be without a request from the other party and without regard to whether the other party has possession of or access to such intelligence.

2. Performance of this obligation as to a particular foreign country requires the recovering party to deliver to the other party a copy of each of the following which it may prepare:

? a. Translations of plain text messages
b. Translations of cryptograms
? c. Strategical and tactical comments appended to translations
? d. Intelligence summaries
e. Crypto-summaries dealing mainly with the titles and effective dates of the foreign country's cryptographic systems
f. Traffic analysis intelligence reports

3. The recovering party is not required, but is permitted, to deliver any of the following:

? g. Translations of plain text messages
? h. Strategical and tactical comments appended to translations
? i. Intelligence summaries.

B. Technical Products

1. As to each foreign country, except those excluded from collaboration and exchange, either party, which makes any cryptanalytic achievement or performs any traffic analysis, will deliver the products thereof to the other party. This will always be without a request from the other party and without regard to whether the other party has possession of or access to such recovery.

2. Among the items intended to be exchanged hereunder are the following:

[redacted]

OGA
EO 1.4.(c)
EO 1.4.(d)

OGA
EO 1.4.(c)
EO 1.4.(d)

[redacted]

3. The following items are not required, but are permitted, to be exchanged:

OGA
EO 1.4.(c)
EO 1.4.(d)

[redacted]

C. Methods and Techniques.

1. As to each foreign country, except those excluded from collaboration and exchange, either party, which in the past has developed or which in the future may develop or which in the future may engage in research in the hope of developing, a method or technique of attack on a communication system of that country, will fully disclose such method or technique, including the administrative organization of the attack, to the other party, or, in the case of research, will fully disclose its plans. This will always be without a request from the other party, and without regard to whether the other party has a method or technique, or is engaged in research in the hope of developing a method or technique, for accomplishing the same or a similar purpose.

2. All of the provisions of the preceding paragraph are subject to the limitations of Paragraph Four of the Basic Agreement.

3. The fact that the disclosing party may have the privilege of using the method or technique or apparatus appertaining thereto on a royalty-free basis, shall not relieve the receiving party of the obligation to pay royalties.

D. Personnel

Each party is authorized, with the consent of the other, to send personnel to work with the personnel of the other party on any task allocated to such other party or for which it may be responsible.

IV Means and Manner of Exchange.

A. Methods of Transmittal

The methods of transmittal of material subject to exchange are provided for in Appendix _____ (Channels for Exchange and Liaison).

B. Time of Making Reports

1. Intelligence, cryptanalytic achievements, products of traffic analysis, disclosures of methods and techniques, and disclosures of plans for research in method and technique, all of which are designated as subjects of exchange in Part III of this Appendix, shall be reported by each party within a reasonable time and by appropriate means, but in every case not later than one month from the date of recovery, discovery or plan,

2. In addition to the foregoing, each party will deliver to the other party a monthly recapitulation of the progress, or lack of progress, made by it on the tasks allocated to it and for which it is responsible.

3. In addition to the foregoing, each party will deliver to the other party a quarterly report of its research in traffic analysis and cryptanalysis not applicable to any immediate problem.

4. The report on withheld methods and techniques provided for in Paragraph Four of the Basic Agreement shall be delivered not later than one month after the date on which it first would become reasonably possible to do so.

C. Reports of Liaison Officers

Each party may forward requests for material subject to exchange to its liaison officers, who will be given full assistance in filling such requests. The liaison officers may also undertake independent studies of operations as a basis for their reports.

D. Forms of Reports

It is recommended that the operating agencies of the parties adopt a uniform system of nomenclature for cryptanalysis and traffic analysis and for designations or titles of communication systems.

D. Standardization of Terminology

1. It is thought that a uniform terminology is desirable, but that as a general principle this uniformity should not be allowed to destroy practices of long-standing which have become familiar to both parties.

2. Cryptanalytic Terms. Every effort will be made to adhere to the definitions and use of terms contained in the ASA dictionary.

3. Traffic Analysis Terms. It is recommended that a uniform terminology be used to describe the various systems of call-sign and frequency working. The following are suggested:

OGA
EO 1.4.(c)
EO 1.4.(d)

Call-sign
- Fixed or Changing
- Station (double or single) or Link

Frequency
- Sending frequency (British: Netz)
- Receiving frequency
- Controlled multinary (British: Star)
- Free multinary (British: Kreis)
- Binary (British: Line)

[redacted]

E. Standardization of Reports

1. The subject matter and kinds of cryptanalytic reports being unpredictably varied, no standardization of cryptanalytic reports is required.

2. Similarly it is recognized that traffic analysis reports should not be rigidly standardized and will change in form and content from time to time. However it is suggested that the following items would cover the general series of reports required and that these designations be adopted to facilitate exchange and classification of material:

a. For Agency and Intercept Station use:

NAC (Net Analysis Casebook): Listing of circuits by case-number
NAD (Net Analysis Diagrams): Circuit Diagrams
NAR (Net Analysis Research): Special traffic analysis reports, such as call-sign studies
NAW (Net Analysis Weekly) : The weekly or monthly report on circuits, together with pertinent data and comments

b. For Agency use only:

TAC (Traffic Analysis Crypt): Traffic analysis studies on the uses of cryptographic systems or on direct traffic analysis applications to cryptanalysis
TAD (Traffic Analysis Diagrams): Circuit diagrams including cryptographic and Order of Battle information

TOP SECRET

TAF (Traffic Analysis Fusion):	Special reports involving the use of Order of Battle and decode material
TAP (Traffic Analysis Personalities) :	Reports of personalities appearing in chatter and simple cryptographic systems
TAS (Traffic Analysis Systems):	Tabulations of cryptographic systems by circuit
TAT (Traffic Analysis Translations) :	Translations of plain language and simple cryptographic systems

As found necessary, other series may be added to the above by either party.

3. It is likewise difficult to standardize the report forms themselves, except for the Net Analysis Weekly which is the basic report and carries routine periodic information. It is recommended that the following form be used:

Case-Number NAW #
Date
C/S system Frequency system
Calls Locations Frequencies Schedules Traffic totals

Heard:
Frequencies Dates

Notes:

V Definitions.

For the purposes of this Appendix, the following definitions are adopted:

Communication: The conveyance of thought by any method (including speech, facsimile and other special means)

Traffic Analysis: The analysis of the radio communication systems of a foreign country with a view toward determining such country's communication methods, procedures, and organization, and the application of that analysis to the related fields of intercept control, cryptanalysis, and intelligence

Traffic Intelligence: All information of an intelligence nature obtainable from the study of foreign radio traffic, by any means short of the cryptanalysis of the text

Cryptanalysis: The total of the processes, other than the processes of traffic analysis, involved in the conversion of a secret communication into plain text, with or without the general system and the specific keys

Cryptanalytic Achievement: Any progress in cryptanalysis.