

2209Z 30-10-1985 PAGE 01

ADD ADS ADC CH CHR CHP SM SMT SMT2 CAC SBOM AMOR-18/11/11

VZCZCSVB178LCA079

RR

DE #3487 3020559

ZNY MMNSH

ZKZK RR SOA DE

R 290557Z OCT 85

FM DSD

TO GCHQ

INFO ZEN/

ZEM

~~SECRET HVCCO~~

4444

SECTION 01

FOR INFO

SMT-031-85

SUBJECT - GCHQ'S NETWORKING AND CRYPT PROCESSING OPERATIONS WITHIN

THE FOLLOWING HAS BEEN CO-ORDINATED BY (CYBER SUPPORT TEAM)
WITH (CRYPT PROGRAMMING SUPPORT TEAM).

1. FURTHER TO THE SIGNAL OF 071044Z JUN 85 RECEIVED FROM

WE ARE CONTINUING TO REVIEW POSSIBLE OPERATIONAL
ENVIRONMENTS FOR CRYPT PROCESSING PENDING THE INSTALLATION OF
MARSIA (CRAY X-MP) EARLY IN 1986 AT DSD.

2. THERE ARE A NUMBER OF AREAS RELATED TO GCHQ'S OPERATIONS AND FUTURE
PLANS ON WHICH WE WOULD APPRECIATE COMMENT; THESE INCLUDE

ALSO, GENERAL OPERATING
REQUIREMENTS SUCH AS MANPOWER, DISK SPACE AND MACHINE POWER ARE OF
IMPORTANCE.

2209Z 30-10-1985 PAGE 02

3. WE HAVE DRAWN UP LISTS OF QUERIES CONCERNING EACH OF THESE AREAS AND HAVE ATTEMPTED TO DIRECT THEM TO THE RELEVANT BRANCH/GROUP. ANSWERS TO THESE WOULD BE OF GREAT HELP TO US IN PLANNING OF OUR FUTURE CRYPT PROCESSING. WE WOULD BE VERY GRATEFUL FOR FORMAL OR INFORMAL COMMENTS OR INDICATIONS OF CURRENT THOUGHT ON ISSUES AS YET UNDECIDED. WE HAVE ALSO INCLUDED A BACKGROUND OF OUR OPERATIONS AT THE START OF EACH SIGNAL.

4. PLEASE NOTE THAT QUESTIONS CONCERNING THEIR RESPECTIVE AREAS HAVE BEEN DIRECTED TO

5. BACKGROUND

A. OUR CURRENT CRYPT PROCESSING AND RELATED CRYPT DATA PROCESSING IS SITED ON A CYBER 175 DUE TO BE DECOMMISSIONED IN MID-1989. OUR CRYPTANALYSIS WILL SHIFT TO MARSIK (CRAY X-MP) AND WE ARE CONCERNED AT THE LACK OF SUITABLE DATABASE MANAGEMENT FACILITIES UNDER FOLKLORE TO REPLACE OUR CURRENT CRYPT DATA STORAGE/RETRIEVAL SOFTWARE. WE HAVE BEEN REVIEWING THE ALTERNATIVES AND THE IMPACT THE VARIOUS OPTIONS WILL HAVE UPON OUR PROCESSING ENVIRONMENT, ANALYST ENVIRONMENT AND NETWORKING REQUIREMENTS.

B. OUR CURRENT CRYPT PROCESSING HAS AS ITS CORE INDEXED SEQUENTIAL FILES BASED UPON CYBER RECORD MANAGER ADVANCED ACCESS PACKAGE. THESE FILES ARE UNDER THE CONTROL OF CRYPT ANALYSTS SUITE OF PROGRAMS WHICH ALLOW DATA TO BE STORED, RETRIEVED, UPDATED AND ARCHIVED, CORRUPTED FILES TO BE REPAIRED AND FILE STATISTICS TO BE COLLECTED. INTERACTIVE AND BATCH ACCESS IS PROVIDED. CAN RETRIEVE SINGLE OR GROUPS OF MESSAGES VIA SYMBOLIC KEYS AND/OR STRING SEARCHING COMMANDS.

FILES STORE CYPHER, WORKING MESSAGES, PLAIN AND CRYPTOVARIABLES. THE ANALYST ENVIRONMENT, ANALYTIC PROGRAMS AND

2209Z 30-10-1985 PAGE 03

AUTOMATIC DATA PROCESSING RELY HEAVILY UPON THIS CENTRAL,
ACCESSIBLE AND MANAGEABLE DATA STORAGE MECHANISM.

- C. IN THE LONG TERM WE WOULD PREFER TO USE A COMMERCIAL DATABASE PRODUCT WITH LOGGING, COMPARTMENTATION, AUDIT TRAILS ETC. SUCH AS IDMS ON IBM OR IM/DM ON CYBER. HOWEVER, THE DATABASE IS ONLY ONE ELEMENT OF THE LARGER PROBLEM OF ENSURING A SUITABLE ANALYST ENVIRONMENT AND INCREASING OUR AUTOMATIC CRYPT DATA PROCESSING CAPABILITIES. OUR CURRENT AUTOMATIC CRYPT PROCESSING HANDLES ONLY HALF OF OUR TRAFFIC.
- D. AS OF EARLY NEXT YEAR WE WILL HAVE THE FOLLOWING EQUIPMENT -
1. CRAY X-MP RUNNING FOLKLORE.
 2. IBM 3033 (UPGRADE DUE 1989).
 3. CDC 175 WITH NOS/BE OPERATING SYSTEM (DECOMMISSION DUE 1989).
- E. WE ARE CONSIDERING THE FOLLOWING OPTIONS IN RELATION TO CRYPT ACTIVITIES -
1. CONVERT ALL CRYPT RELATED WORK TO MARSIK.
WHILE THIS OPTION ALLOWS CENTRALIZATION OF THE DATA, PROGRAMS AND USERS WE BELIEVE UTILITIES AND FOLKLORE DATA BASE WOULD ALL BE INADEQUATE AS REPLACEMENTS FOR OUR CURRENT DATA STORAGE MECHANISMS.
 2. CONVERT OUR CRYPT DATABASE AND DATA PROCESSING TO OUR IBM.
IN THIS AREA WE HAVE BEEN REVIEWING ALSO THE POSSIBILITY OF WRITING
 3. CONTINUE WITH OUR CRYPT DATABASE ON A SMALLER FRONT-END CYBER LONG TERM.

2209Z 30-10-1985 PAGE 04

THIS OPTION WOULD ALLOW INTEGRATION OF THE CRAY WITHIN OUR
CURRENT OPERATIONAL ENVIRONMENT, PLUS THE ABILITY TO RE-ACTIVATE
CURRENTLY INACTIVE CRYPT SYSTEMS . HOWEVER, THE SUPPORT
OF AN ADDITIONAL MAINFRAME IN THE LONG TERM HAS DISADVANTAGES.
ALSO NETWORKING ISSUES NEED TO BE RESOLVED.

#3487
NNNN