78

CH/02-86

ADC

Copies : ~~ADD~~ – – – ADD
ADS
SM
CA
CAC

OUTLINE OF OBJECTIVES FOR CH

The attached paper is an attempt to bring together issues affecting CH and provide an outline of objectives for the future for long term planning purposes. It expresses the opinions of CH staff and is submitted at this time to be used as the basis for coordinating the work of SM and CH in the future.

No apologies are made for the expressions of "motherhood" in the paper.

CH

11 February 1986

78 (A)

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

COPY NO. 2 OF 7 COPIES

PAGE NO. 1 OF 3 PAGES

ANNEX to
CH/02-86 of
11 February 1986

OUTLINE OF OBJECTIVES AND OBSERVATIONS ON THE FUTURE FOR CH PROCESSING

1. MARSIK

i) MARSIK should be used only as a cryptanalytic machine. It should not be used for data processing or hold the CH data base. Supercomputers are tending to become number crunchers more and more and inevitably will be upgraded or replaced on a regular basis. DSD should not be required to convert whatever preprocessing software they use whenever a new crypt computer is bought.

ii) Front end processing - a front end processor needs to be acquired to enable this to be achieved. Whether this should be in the long term another CDC machine, IBM or an expanded LIBRETTO is for someone else to judge. A lease of a small CYBER to allow time for front end conversions beyond 1989 will probably be necessary.

iii) There are reservations about LIBRETTO being suitable as a front end machine - it is believed to be well occupied these days and with the likelihood of high capacity systems coming along in the future, it will quickly fill up if it isn't close to that now.

iv) Front end processing should be portable and written in the expectation that it will stand the test of time. It should be designed in as general a way as possible in the expectation that it will remain in place after the demise and replacement of the CRAY.

v) All front end processing should be controlled by SM although for follow-on crypt processing should be controlled from within CH. CH should ensure that any automatic processing system designed from now on is "fully portable" and written in such a way that it works on the CYBER but can be transferred without any need for rewriting on any future front end processor. DSD believes that is a superior preprocessing system to any in use and should be retained (converted for portability). This would make DSD independent of the other centres but be consistent with the overall policies of our partners.

vi) FOLKLORE is expected to be phased out after another five years. DSD should ensure that once FOLKLORE is superseded any new system can be adopted in parallel with and at the same time as the other agencies. No rewriting of any C/A software should be contemplated for any successor C/A machine.

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

2. CN Implications

i) CN relies on CH data processing for its statistical records. It says it does not need to conduct . Front end processing should be arranged to give CN access to its data and should be tied in with current work on .

ii) As data has to come off the CYBER by 1988/89 and assuming CH has its data base on a new front end processor, CN will have to get access to that part of the front end processes it requires. Some difficulty might present itself here in respect to access to crypt variables.

3. SM Implications

i) SM has to date left it that CH handles all crypt data base and crypt processing. This resulted in the undesirable event that CH set up and the and related suite of front end processing systems. If the CYBER is to be phased out by 1988/89 and if a new front end processor is to be acquired to replace the CYBER, work should start soon to have the automatic processing fully rewritten by this time. SM should be involved with CH in making this automatic processing "fully portable" for use on the CYBER or its successor. The best approach would seem to be that CH while SM so that by the time CYBER is phased out all front end processes are rewritten with SM in charge of this aspect of the work. One way this could be done is for SM support to be provided to CH either in the posting of one or two staff to CH for a given period, or a halfway house, such as exists with be established for this purpose.

4.

i)

ii)

a)

b)

c)

78(c)

5. Other considerations such as the system to be used for computer transfer (Transfer vis-a-vis) and the speedy resolution of the procedures for exchange of crypt information/software need to be resolved. The access of CHT to data on MARSIK will be achieved by the installation of a terminal in CHT, but the use of this system relative to the system in use in the CHT laboratory, need to be examined. One matter that might be considered is whether the CHT tasks all be centralised in one processing area in CHT (a separate paper has addressed the matter of CHT processing).

6. One final point is that provision should be made in communications planning for all intercept collected at to be passed to DSD, which in the case of tasks such as will mean that both will be forwarded to DSD irrespective of . This is necessary to allow CH to be able to or when a machine changes or for whatever reason. This is not meant to take over the in any way and should not be seen to be an attempt to do so.

and the cost?