18

33/7/1
~~37/2/42~~

Director

Copies to: ADA (less attachment)
ADD
ADS
ADQ
CA
CC
CH
CN
SM
AGR (less attachment)

1. The attached paper has been prepared by CHR. It is a detailed restatement of the case for the major upgrade of DSD computing power in support of cryptanalysis and sets out the operational aim underlying this upgrade as seen by C Branch. In March 1982 the upgrade project was named Project LOBSTER.

2. The requirement is set against the background of the aims of cryptanalysis at DSD, the development of cryptographic knowledge and techniques in the outside world, the considerable upgrades in computing power at NSA and GCHQ, and the collaborative arrangements (and their benefits) existing with those agencies. The immediate context of DSD's current crypt effort with current computers against current targets is then discussed, along with the target trends which are now discernible. The conclusion, which is that the acquisition of the LOBSTER upgrade should proceed without further avoidable delay, depends on the following considerations.

JUSTIFICATION

3. BACKER has been fully loaded (3 shift working) for about a year. Processing of current operational targets is at present performed satisfactorily, but this situation could change due to slight shifts in cypher usage by DSD's major targets. There is no spare capacity now, and will not be until the next upgrade is installed to cope with target developments. Indeed, at best, a gradual degradation of capability relative to DSD's current tasks is to be expected from now on. Further, any projected expansion of DSD cryptanalytic effort is circumscribed by currently available computer resources; one possible new target is a system which, if properly used, would be inaccessible giving our limitations in computing power.

4. There is little or no reserve capacity to cope with an emergency. If a crisis were coupled with an upgrade of Comsec practices it would become very difficult indeed to perform an essential part of DSD's mission.

5. Emergencies apart, any substantial change in target systems, eg to some of the newer cipher machines on the market, could require increases of at least an order of magnitude to recover the present level of performance. Such changes must be considered more and more probable as time goes on, as a result of increased Comsec awareness, improved and cheaper technology, and increased sales effort by commercial manufacturers.

6. Apart from the need for greatly increased computer power (paras 3-5 above) the likely advent of a greater variety of more difficult target systems will create a correspondingly increased need for operational software. The present CYBER system is software-incompatible with the new computers being procured and installed at NSA and GCHQ, and so requires that all crypt developed and programmed there have to be reprogrammed at DSD. A new computer which offered program compatibility would provide virtually immediate access to a large body of software which would contain programs either completely adapted to DSD needs or providing groundwork for writing such programs. To obtain this enormous advantage for the future a comparably sized machine with compatible operating system is needed. A bonus is that the operating system (FOLKLORE) currently in use by NSA and GCHQ was designed for cryptanalytic purposes

7. For DSD to maintain its collaborative relationship with NSA and GCHQ it must be able to pull its weight in the cryptanalytic field. The relationship brings considerable benefits and it is present policy to maintain it. The projected increases in computer power at NSA and GCHQ throughout the 1980's and beyond show that without a considerable upgrade DSD's effort will become (more) insignificant in comparison. And of course these large projected increases are based on estimates of future requirements which must be strongly correlated with DSD's own requirements. We are not seeking to upgrade our capability merely to keep up with the larger centres.

8. It is 5 years since the last upgrade, and in 1985/86 it will be 7 years; if the next upgrade is to be sufficient for a similar length of time, the target increase of power must be what is considered necessary towards the end of the decade. Of course an intermediate upgrade would permit a smaller initial increase.

9.

Assuming that DSD does not in the near future obtain such a machine, a (conservative) factor of 2 is incorporated in the figure for the end of the decade; a final estimate for this period is a 30 fold increase in power over that provided by BACKER.

CONCLUSION

10. It is concluded that an upgrade of computer power by a factor of 30 is a conservative estimate of what is required at the end of the decade, a factor of 10 in 1985/86 if the acquisition is staged; that 1985/86 is the latest possible

date for first-stage acquisition to avoid undue loss of effective capacity, that compatibility of operating system, programming language, and comparable rate of increase in computing power vis-a-vis NSA and GCHQ is essential for the maintenance of effective collaboration. The acquisition should be given top priority.

RECOMMENDATION

11. All possible steps should be taken to ensure successful procurement of a computer upgrade satisfying the above requirements in 1985/86.

ADC

23 March 1983