In considering the reliability of cipher machines, we find

that modern engineering and cryptographic techniques have accom-

plished this to a satisfactory degree. Although the machines are

complex, their reliability can be assured by having properly trained

personnel to operate and maintain them. Accuracy is also one of

the elements of reliability and a good cipher machine can yield a *very*

higher degree of accuracy *and* ~~or~~ completeness of text, ~~than can a code~~

~~system.~~ A mistake in one or two code groups/may obscure, alter,

in the case of a code system

or render unintelligible the meaning of the whole message, but in

cipher systems, ~~(often)~~ wrong letters may *usually* be corrected, or missing

letters supplied. The use of the wrong key or wrong "setting"

whole

may, of course, prevent the decipherment of a message *or a whole part, in*

case the message consists of two or more parts, but this doesnt often happen.

Let's now consider the security angle. If reliability were

the only or the most important factor, code would be preferable

to cipher for all echelons of command because the simplicity of

a code book is to be preferred to the complexity of a large cipher

machine. However, unenciphered code is not sufficiently secure for

the communications of the highest echelon and headquarters, and

when a second step of encipherment is added, it practically destroys

the simplicity features of a code. In a properly designed cipher

machine, embodying sound cryptographic principles, the single

step encipherment process can yield cryptograms of very great

security. In a good code system, however, the solution of one or

even of several messages does not entail the immediate breakdown

of the entire system, with the consequent ability to read all mes-

sages, as is usually the case in a cipher system. A good cipher

system may be compared to a library housed in a large structure

of many rooms with all doors and all windows securely locked. If

an intruder can force an entry into the structure, he will find a

master key which will open all the locks and give him access to

all the books in the library. A good code system (especially

a two-part code) may be compared to a library housed in a similar

structure, but no two locks are alike and no master key is avail-

able or can be made. Therefore, the lock on each door must be

worked at patiently as a separate problem. Thus, although the

intruder may force his way into one room, this gives him access

to only a small part of the library; in order to read all the books,

he must force his way into each room, which takes much time, since

each lock presents a separate and special problem. Code books,

of course, can be rendered useless by compromise. Actual possession

for a long period of time is not necessary; methods of rapid photo-

graphy may be applied and a book of several hundred pages copied

in a few minutes.

As regards rapidity, the speed of operation of a cipher machine leaves even simple unenciphered code far behind in the matter of rapidity.

In the matter of flexibility, we find that a cipher machine is much more flexible than a code and can be used for all sorts of messages. In a code containing words, phrases, and sentences prepared for a specific type of communication, rewording the original text as written by the originator is often necessary, if the words, phrases, and sentences in the code book are to be used; otherwise, the original wording must be encoded word by word, or even syllable by syllable.

Finally, with respect to economy, whether expressed in terms of money or manpower, cipher systems are more economical than code systems for high and intermediate echelon communications. A single clerk operating a rapid cipher machine can turn out 10 to 15 times as much work as one operating a code system; furthermore, codes must be prepared, printed and distributed--steps which take much time and labor to effect.

It's clear that high-grade and medium-grade systems should include all or as many as possible of the five factors discussed