PL 86-36/50 USC 3605

[redacted]

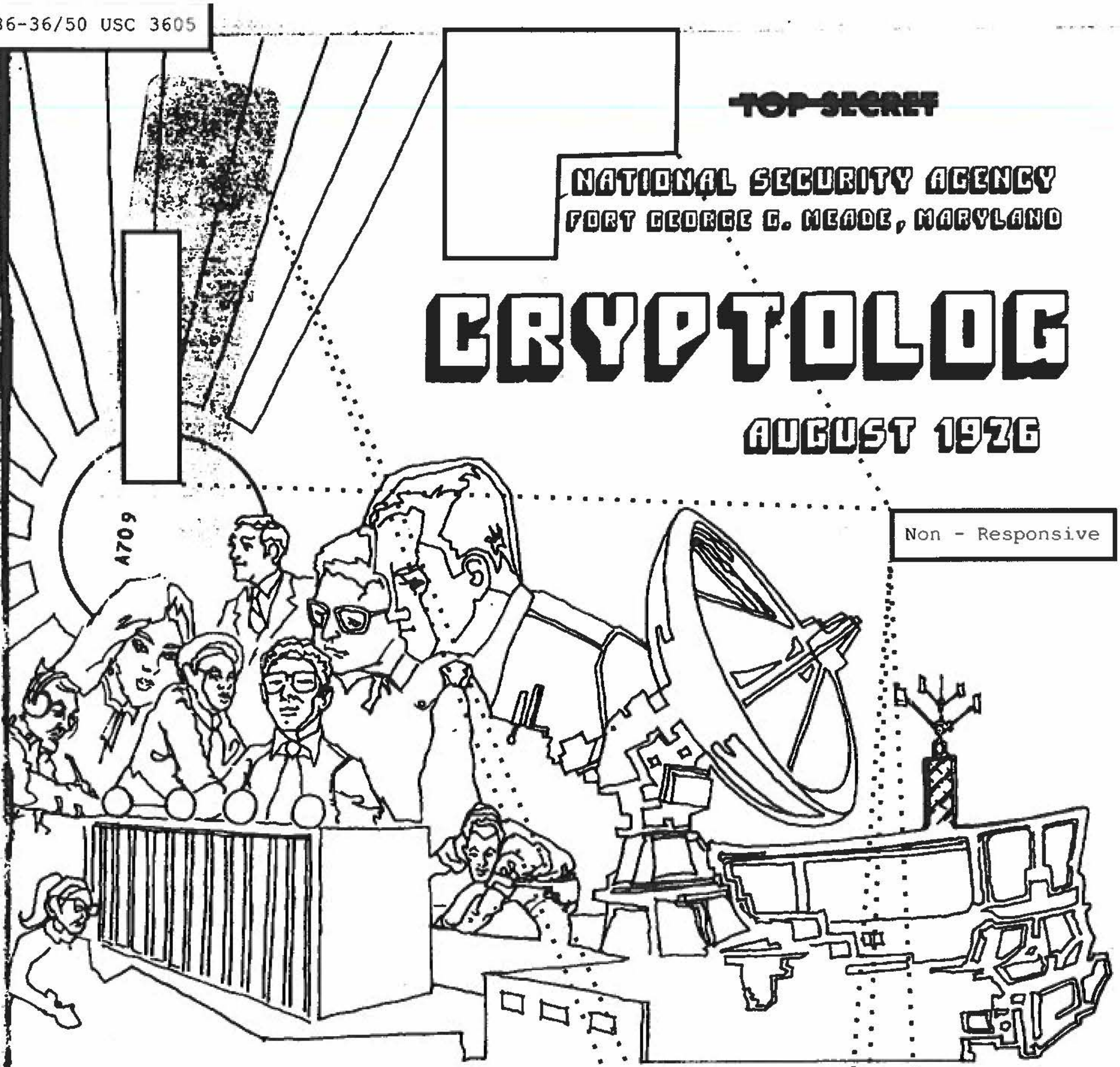
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUGUST 1976

[redacted]



Non - Responsive

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

Not A Final Version - Proposed Release for MDR Case # 109434

[redacted]

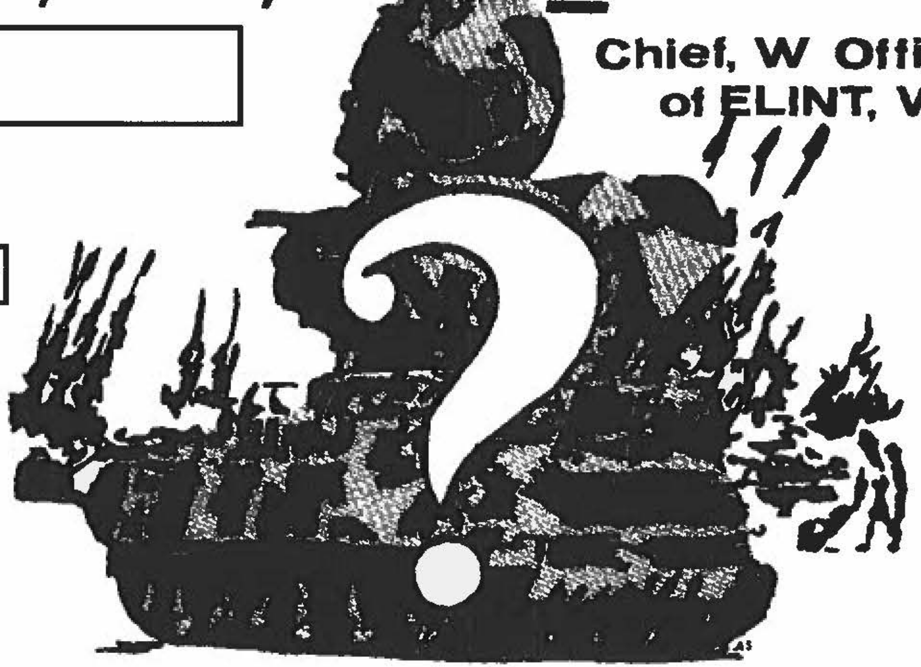
Non - Responsive

YES, DON, THERE <u>IS</u> AN ELINT!

[redacted]

PL 86-36/50 USC 3605

Chief, W Office of ELINT, W2



Yes, Don, there *is* an ELINT! Because you don't recognize it, doesn't mean it doesn't exist. Your NSA colleagues who plant its seeds, who nurture its growth, who channel its energies, and who harvest its fruits resemble in many ways the more "normal" NSA employee. You might, therefore, have as much difficulty recognizing an ELINTer as you do ELINT, but, believe me, they exist too.

In the April issue of CRYPTOLOG you asked if the real ELINT would stand up.* You indicated that it appears to be a shadowy operation and that many COMINTers would like to know what it is all about. Happy to oblige. We ELINTers have been so busy practicing our science (art?) that we didn't notice all of you waiting to be enlightened in the ways of ELINT -- perhaps to join the fun. We're a proud bunch who know we are an NSA minority specialty group with an important job to do, and we think that we're doing it rather well. We can do it even better, and we are working at that. We will attempt to throw light into the shadows, remove mystery, and minimize jargon.

Formal definitions of ELINT do in fact include all non-communications electronic emission intelligence except lightning and nuclear emissions. As practiced at NSA, our energies are devoted primarily to ELINT associated with potentially hostile military-threat weapon systems. Yes -- this represents the analysis of weapon systems primarily through their radars, radar-like devices, weapon-control electronics, jamming signals associated with all of these, and the jamming of communications signals.

NSA partitions ELINT into two classes: Operational ELINT and Technical ELINT. (Telemetry -- TELINT -- is the province of W1. Perhaps they will tell you about that sometime.) Since October 1974, most Operational ELINT activities are handled by the appropriate A, B, or G Group analytic elements. Technical ELINT is focused in W's Office of ELINT, W2. What is the difference? Simply stated, the following illustrates the products of the two types of ELINT information.

<u>*Technical ELINT provides*</u>:

- *signal descriptions* -- All the parameters of a signal that can reasonably be defined are collected and measured to a degree commensurate with our capability and the degree of military interest. These measurements provide the ingredients for analysis of the emission characteristics *and assessment* of the emitter.
- *emission characteristics* -- The signals (and combinations of signals) are analyzed from signal descriptions. The character of the

* Don Bulla, "Will the *Real* ELINT Please Stand Up?", *CRYPTOLOG*, April 1976, p. 5.

EO 3.3b(3)
PL 86-36/50 USC 3605

emissions is determined to establish how best to exploit them and to gain insight into the degree of threat they may represent

- *modes of operation*

[redacted]

- *emitter functions*

[redacted]

- *weapon-system associations*

[redacted]

[redacted]

So what does Operational ELINT provide that has not been discussed? On those emitters described by Technical ELINT,

Operational ELINT provides:

- *emitter deployment*

[redacted]

EO 3.3b(3)
PL 86-36/50 USC 3605

PL 86-36/50 USC 3605

[redacted]

Since space is limited, and since the author's current responsibilities encompass Technical ELINT, the remainder of this article will be devoted to Technical ELINT. Perhaps a representative of A, B, or G Group will elaborate on Operational ELINT in a subsequent issue of CRYPTOLOG.

As outlined earlier, Technical ELINT is in general aimed at:

- understanding military threat weapon systems;
- [redacted]
- providing similar information on jamming signals.

While the following remarks are neither comprehensive nor intended to show the "only" way that things happen in Technical ELINT, they should serve to illustrate the basic activities of Technical ELINTers.

- *Requirements definition* -- Requirements are generated by the military operating commanders expressing their need for information on a potentially hostile new emitter (for example, a new radar) or by their associated service intelligence agency analysts who are aware of the new radar and generate requirements on behalf of the operating commanders. These service intelligence agencies are the:
    - *Foreign Technology Division (FTD)*, for the Air Force;
    - *Missile Intelligence Agency (MIA)*, for the Army's large missile systems;
    - *Foreign Science and Technology Center (FSTC)*, for the Army's general battlefield systems and electronic-warfare intelligence; and
    - *Naval Intelligence Support Center (NISC)*, for the Navy.

  The need for ELINT information is generated by and through these service centers and forwarded to DIA for consolidation and validation. DIA, in turn, levies the requirements on NSA.

  The W2 Requirements/Collection Managers (with the appropriate analysts) convert the DIA need for ELINT information into specific collection/processing/analysis guidance detailing the character of the data needed from the world-wide variety of collection resources. Working with V3, W2 has the data needs and reporting instructions forwarded to the collectors who can contribute -- often these instructions are specifically tailored to their ability to contribute.

- *Collection and collection management* -- W2 performs both collection and collection management functions. [redacted]

- *Processing and processing management* -- As with other steps in the ELINT procedure, processing of collected data is accomplished in a variety of ways. Processing is defined as the step between signal collection and analysis (to be defined later). Processing is accomplished at the point of collection, at theater processing centers, and Hq NSA. Again, NSA ELINTers have considerable impact on the quantity, quality, and location of ELINT processing.

- *Analysis and analysis management* -- ELINT analysis is defined as that part on the ELINT production cycle wherein analog and digital data is converted into intelligence information. Hq NSA ELINTers *perform* a substantial level of analysis; directly manage analysis by contractors on specialized problems; provide general analysis assistance and management to collectors and processing centers; and are directly involved in the management of analysis assistance being provided by the service science-and-technology centers (FTD, MIA, FSTC, and NISC) by formal agreement between NSA, DIA, and the centers. The analysis and analysis management function presents considerable technical and managerial challenge, but the challenge is being met with reasonable efficiency.

- *Reporting and reporting management* -- The best intelligence information is absolutely worthless until it is reported, and used, by those who take action on the basis of such information. Thus, since we cannot force the customers to use our product, our challenge is to report all potentially useful information in as complete, timely, and readable a format as possible, with the important ele-

EO 3.3b(3)
PL 86-36/50 USC 3605

ments highlighted. With the vast variety of processes and procedures that lead up to the dissemination of an end-product report (including a variety of field reporting procedures), it is very difficult to keep the operation glued together. Currently, there is a very complex array of "field" reporting procedures and vehicles. There is also currently, however, a comprehensive reporting procedure *study* underway, with the objective of simplifying the process. As in the song, we have "High Hopes."

The foregoing paragraphs are designed to give you a very quick survey of ELINT -- especially Technical ELINT -- as practiced at NSA.

[redacted]

[redacted]

So what have we done for you *lately?* Plenty! -- most of which should not be revealed in a broad-distribution publication. Come to us with your clearances and need-to-know intact and we will be happy to tell you.

Yes, Virginia (I mean Don), there *is* an ELINT, and the real ELINT should be happy to stand up. To the benefactor of ELINT [redacted] goodies provided by ELINTers are more valuable than gifts he received from Santa Claus. We ELINTers work so closely with our electronic warfare "customers," contractors, a rather broad range of COMINTers and many others that we sometimes lose sight of the fact that we are (in number) a small part of the SIGINT effort and that we are well known to only a relatively few. We thank you for your reminder that we do need to pause occasionally for a bit of public-relations exposure, even within the Agency. Hope this short discussion helps. Want to know more? Contact us.

~~(SECRET — HVCCO)~~

[redacted]

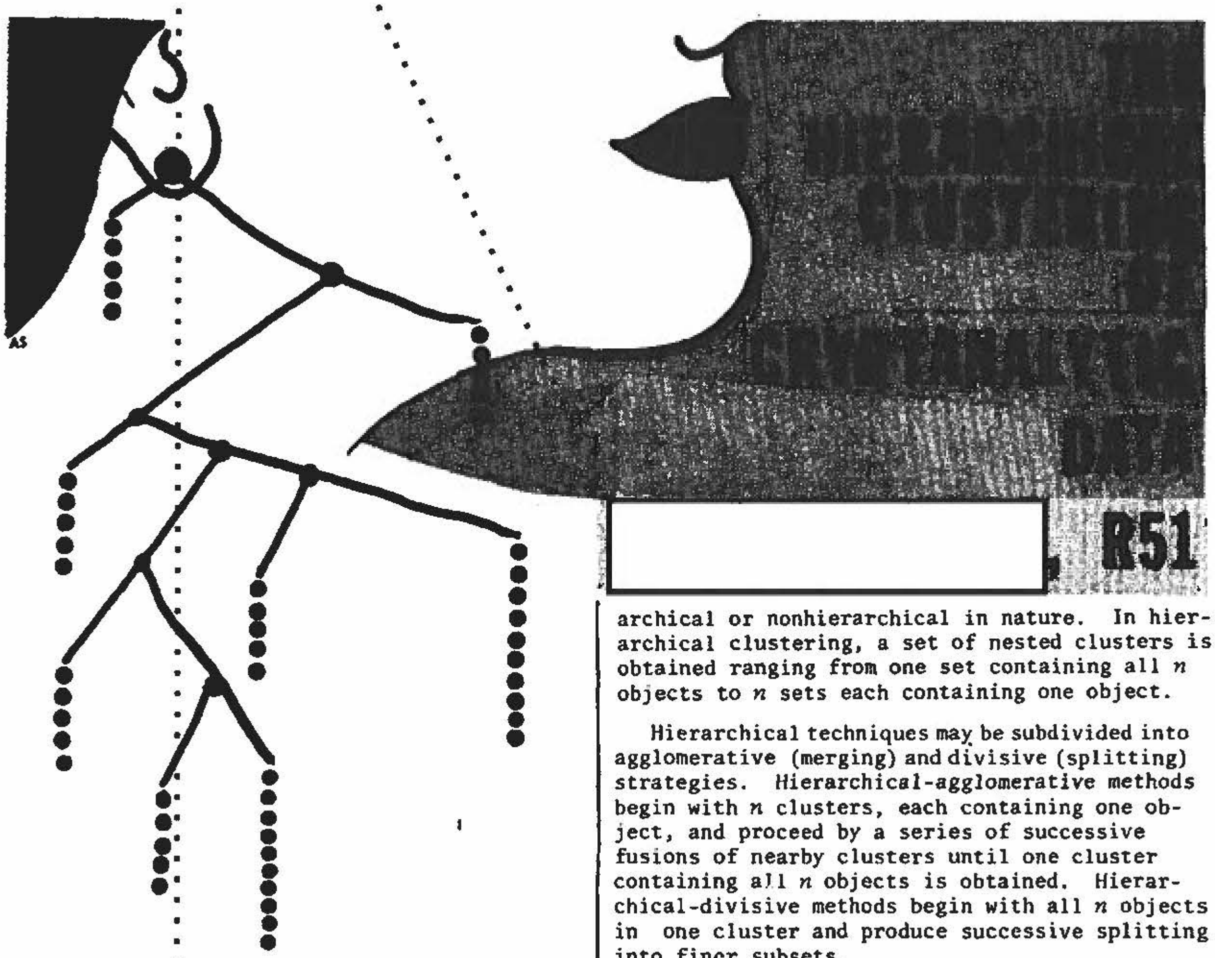
Non - Responsive

Non - Responsive

[redacted]

Non - Responsive

PL 86-36/50 USC 3605



THE HIERARCHICAL CLUSTERING OF CRYPTANALYTIC DATA

[redacted], R51

During the past year, CADRE, a P1/R51 group headed by [redacted] has been investigating cluster analysis and multidimensional scaling and has been assessing the relevance of those techniques to Agency work. A number of computer programs implementing those methods have been acquired and adapted to Agency computers.

Two hierarchical clustering algorithms, HICLUST and PEP-1, have proved to be quite useful in a variety of Agency problems. CADRE has studied several cryptanalytic applications with highly encouraging results. For example, for matching alphabet profiles, HICLUST and PEP-1 have been demonstrated to be substantially better (in the sense of producing a more accurate result) than the XIBAR method, the traditional Agency approach based on cross I.C. values. Furthermore, recent R51 research suggests that the cross I.C. measure itself may be significantly inferior to other types of comparisons such as correlation coefficients, normalized dot products, and Euclidean distances.

Cluster analysis seeks to categorize *n* objects, each defined in terms of values associated with *p* variables or attributes, into *g* homogeneous subsets (clusters). Clustering algorithms may be classified as being either hierarchical or nonhierarchical in nature. In hierarchical clustering, a set of nested clusters is obtained ranging from one set containing all *n* objects to *n* sets each containing one object.

Hierarchical techniques may be subdivided into agglomerative (merging) and divisive (splitting) strategies. *Hierarchical-agglomerative* methods begin with *n* clusters, each containing one object, and proceed by a series of successive fusions of nearby clusters until one cluster containing all *n* objects is obtained. Hierarchical-divisive methods begin with all *n* objects in one cluster and produce successive splitting into finer subsets.

HICLUST (HIerarchical CLUSTering) is a hierarchical-agglomerative method using the nearest-neighbor and farthest-neighbor algorithms. PEP-1 (Probablity Evaluated Partitions, Version 1) is a hierarchical-divisive method using graph-theoretic concepts. HICLUST was written at Bell Labs; PEP-1 is a member of the Guttman-Lingoes Nonmetric Program Series (University of Michigan Psychology Department).

All clustering algorithms are designed to produce clusters regardless of the structure of the data. Most clustering techniques make assumptions concerning the number and shapes of clusters in the data. HICLUST and PEP-1 attempt to produce clusters using the intrinsic structure of the data, and both programs (especially PEP-1) generate statistics to help the analyst differentiate clusters from random groupings.

Both HICLUST and PEP-1 analyze a square symmetric matrix whose entries measure either the distance or the likeness between objects. Both programs are very easy to operate and are available on LODESTAR, the IBM 370, and the R5 6600.

Here is an example which illustrates the type of situation in which PEP-1 and HICLUST have proved to be valuable. Suppose a cipher stream is suspected of having been generated by a periodic polyalphabetic system with a 50-wide key, and the objective is to determine the number of different alphabets (or different slides of the same alphabet) used and the key positions that are enciphered with the same alphabet.

Such a problem was solved in 1974 using statistical programs available on the RYE computer system. In 1976 this cipher was reexamined by CADRE using modern cluster analysis and multidimensional scaling methods. The CADRE techniques easily (and *perfectly*) determined the number of alphabets used and the key positions enciphered by the same alphabet. A hierarchical-clustering representation of the results from HICLUST and PEP-1 is shown in Fig. 1. The clusters can be interpreted in a more meaningful fashion by means of the matrix in Fig. 2.

The statistics generated by PEP-1 and HICLUST, coupled with Fig. 2, clearly establish the validity of the clustering.

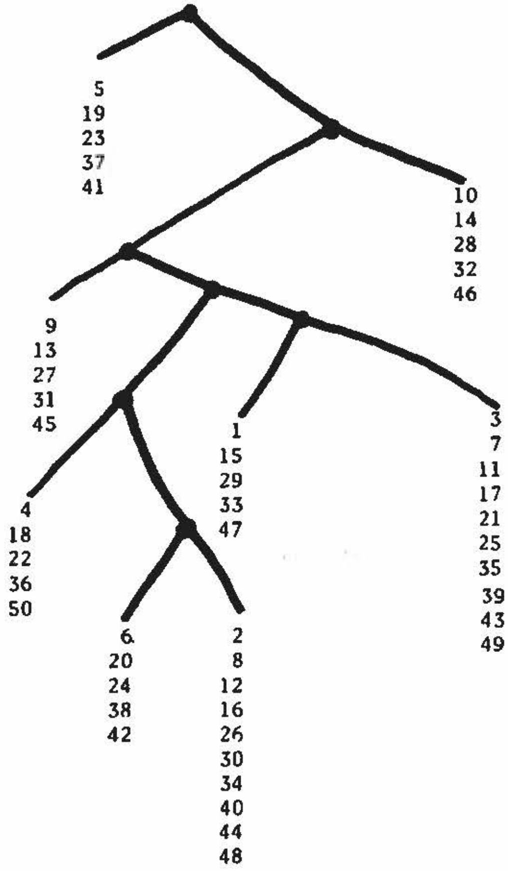


Fig. 1. Hierarchical clustering of PEP-1 and HICLUST results

More details about this example (and about additional examples involving typewriter-random key generation and codebook reconstruction) can be found in the recently published R51 paper, *The Hierarchical Clustering of Cryptanalytic Data and Comparison with Multidimensional Scaling*, by [redacted] and [redacted] (R51/TECH/01/76, dated 5 March 1976). (You may obtain a copy of this paper by calling Mrs. [redacted] in the R51 Library, Room 3N101-3, x4730s).

CADRE is investigating more sophisticated clustering approaches and also multidimensional scaling methods (for the case in which a paradigmatic structure, such as a linear or circular ordering of the points, is sought *instead of* clusters). To further extend its research effort, CADRE is actively seeking data sets (cryptanalytic or other) from numerous Agency offices. Inquiries about the computer programs used by CADRE or questions about submission of data sets for analysis should be directed either to [redacted] R51, 5530s, or [redacted] R51, x5228s.

Slide	*Key positions enciphered by each slide*							
1	1	-	15	-	29	33	-	47
2	2	-	16	-	30	34	-	48
3	3	-	17	21	-	35	-	49
4	4	-	18	22	-	36	-	50
5	5	-	19	23	-	37	41	-
6	6	-	20	24	-	38	42	-
7	7	11	-	25	-	39	43	-
8	8	12	-	26	-	40	44	-
9	9	13	-	27	31	-	45	-
10	10	14	-	28	32	-	46	-

Fig. 2. Interpretation of cluster structure after revision

~~SECRET SPOKE~~

[redacted]

Non - Responsive

[redacted]

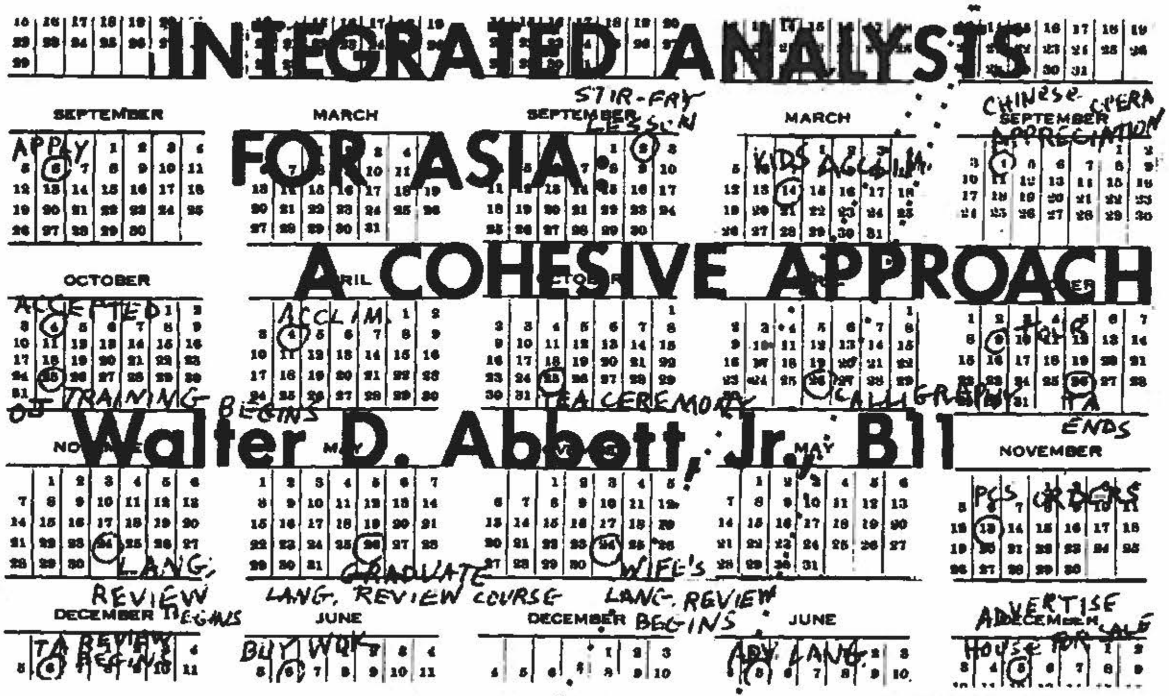
Non - Responsive

Non - Responsive

Non - Responsive

INTEGRATED ANALYSIS FOR ASIA: A COHESIVE APPROACH

Walter D. Abbott, Jr., B11



[redacted]

On the other hand, in spite of the resource decrement, the intelligence requirement continues. SIGINT remains our first line of defense, and it is incumbent upon us to respond to this charge with all the resourcefulness we can muster.

[redacted]

[redacted]

EO 3.3b(3)
PL 86-36/50 USC 3605

[redacted]

[redacted]

If you are still with me to this point, please don't send me any letters saying that we are already doing all of this. For each case you cite wherein the full objective has been achieved, I can cite two or three wherein the objective was either ignored or effectively undermined, and that is not my purpose in any case. What I am earnestly requesting is that this Agency recognize an area which will be of vital importance in the future, and take every reasonable step to insure we are up to the challenge. If we are to succeed, as succeed we must, we need to be innovative, thorough, deliberate, and, above all, cohesive in our integrated analyst program management; and it is within our capabilities to do so. We, as an Agency, should not settle for anything less.

~~(SECRET UMBRA)~~

Non - Responsive

Non - Responsive

Non - Responsive

[redacted]

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

[redacted]

Non - Responsive

[redacted]