

MDR Case # 54778

11 1 1

TOP SECRET

CEVPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. II, NO. 12	DECEMBER 1975
PUBLISHER	WILLIAM LUTWINIAK
	BOARD OF EDITORS

Editor in chief	Arthur J. Salemme (5642s)
Cryptanalysis	(8025s) P.L. 86-36
Language	
Machine Support	(3321s)
Special Research	Vera R. Filby (7119s)
Traffic Analysis	Frederic O. Mason, Jr. (4142s)

For individual subscriptions send name and organizational designator

to: CRYPTOLOG, P1

TOP SECRET

-SECRET



The following three articles deal in various ways with the publicity given in the British and American press and on television to F. W. Winterbotham's book "The Ultra Secret." The first article, by Brigadier John H. Tiltman, deals with the accuracy of the statements in the book and the degree of harm done by them. The second article, by P. W. Filby, is a review of the book as assessed by a member of the team of specialists who worked the German diplomatic problem. The third article, by M542, gives a word of advice to those who might now be tempted to tell everything they know.

P.L. 86-36

A PERSONAL COMMENT By Brigadier John H. Tiltman, P1

When Winterbotham's book was first published late in 1974 in England, some members of NSA who had served at Bletchley Park during World War II, on reading early reviews, assumed that it was officially authorised. This was definitely not the case. Its publication was strenuously opposed by British responsible authorities, who took legal advice on the probable consequences of prosecuting the author under the British Official Secrets Act. They were advised that prosecution could not be effective without the case going to court and evidence produced that British national security had been damaged by the book's publication with consequent public disclosure of more current intelligence activities. They therefore decided that legal action would probably do more harm than good.

Another and perhaps a decisive factor making prosecution unlikely to succeed was the publication in France in 1973 of Bertrand's book *Enigma, ou La Plus Grande Enigme de la Guerre* 1939-1945. This revealed for the first time the fact of an analytic success against the Enigma and was decisive in the discussions between Deputy Director NSA and Director GCHQ on the matter of whether to attempt to restrain Winterbotham and his publisher.

I am not alone in believing that an early official public description (perhaps a joint US-UK statement) of the basic facts of the wartime exploitation of the intelligence derived from the solution of the Enigma keys might have mitigated the damage done to security. Perhaps this could have been strengthened by a further

December 75 * CRYPTOLOG * Page 1

SECRET

HANDLE VIA COMINT CHANNELS ONLY

boper and Daniel Davidson

statement that the revelation of technical details of the methods of solution would be resisted indefinitely. I realise however that there must be other valid arguments which persuaded the responsible authorities not to take such action.

I myself took no part in the solution of Enigma keys in Huts 6 and 8, nor in its exploitation in Hut 3, but I am, I believe, the only person around who was on the directorate level at Bletchley Park during the war and had a hand in many of the policy decisions made regarding the production and use of the intelligence derived.

The book is poorly written and very inaccurate in some areas where I know the facts. The references to the early history of Enigma solution and to the activities of the staff of Hut 6 (who performed the cryptanalytic part of the enterprise) are hopelessly wrong. It is difficult to understand how the author who had considerable responsibilities for the organisation and distribution of Enigma intelligence could have been so completely ignorant of the technical side of the operation. He doesn't know the difference between the Enigma (a rotor machine), other German ciphers, the Japanese high-grade diplomatic machine (the "Purple," a totally different kind of machine), and the Japanese Fleet general cipher (a codebook and additive hand system). His remarks about the "Bronze Goddess" appear to be a complete invention.

Some people gather the impression when they read the book that the author greatly magnifies his own part in the winning of the war. I give an example from my own experience. To quote some passages, "It was at this point that Menzies told me he had decided to hand over my shadow OKW in Hut 3 to the General Administration at Bletchley. One never knew where one stood with Menzies. He softened the pill by confirming me as his deputy, . . ." (p. 87). "Despite the loss of my personal control of Hut 3 and the shadow OKW, I still had direct access to it when required. I was never told by Menzies the real reasons for the takeover, . . ." (p. 92). The facts are that I reported to the Director of Military Intelligence at the War Office, that Curtis, the War Office representative in Hut 3, in conjunction with Humphries, the corresponding Air Force representative, had on two separate occasions gone behind my back to recommend reorganisation of Hut 3 under their own more direct control. In consequence, a SIGINT Board meeting was called with General Menzies in the chair and consisting of the three Service Directors of Intelligence and Director GCHQ. At this meeting it was decided to withdraw Humphries, Curtis, and the naval representative.

I knew Winterbotham slightly and flew with him to Paris on the occasion of one of my official visits to France in 1940. His outstanding achievement was the establishment of SLUs (special liaison units) for the dissemination of ULTRA to commanders in the field. I have no reason to doubt that he records this faithfully. He gives rise to feelings of discomfort, however, when he describes his relations with the more high-ranking recipients of his wares. It appears that Montgomery must have treated him with less courtesy than others and consequently he feels sure he himself could have fought Montgomery's battles far more efficiently!

In view of its general inaccuracy, especially when touching on technical matters, I believe the book, taken by itself, does no harm. This cannot be said for the side effects it touched off. The first review I read was in the Washington Post by Al Friendly, who himself served in Hut 3. He headlines his review "Confessions of a Codebreaker." He gives the impression that for a great part of the war every telegraphic order issued by Hitler was currently on the desk of the Prime Minister and concerned Allied commanders. This is simply not true. Such a picture takes no account of the many difficulties of the operation, the decisions to be taken on insufficient evidence as to priorities of attack on some keys to the exclusion of others, the many failures and delays, the early misunderstanding as to the real meaning of messages, etc. The general success of the project was as much a triumph of organisation of the large-scale attack as of the ingenuity and persistence of the cryptanalysts, especially the mathematicians.

Perhaps the most objectionable of the reviews was a long article in one of the London Sunday newspapers by Peter Calvocoressi. He was an important figure in Hut 3, presumably recruited by Winterbotham. He is now, I believe, managing director of Penguin Books and was the joint author of a distinguished history of World War II. His article is an extremely well-written description of life in Hut 3, but he has gone further than anyone else in including a photograph of the German Service Enigma and in mentioning the Bombe. I believe this was the first time a picture of the service Enigma appeared in public print. Not even Bertrand in his book Enigma gives a photograph of the machine. I am quite unable to understand Calvocoressi's arrogant assumption that he can say what he likes in public now that Winterbotham's book has appeared. I hold the view that everyone who worked in Bletchley Park is still under a moral obligation not to disclose secrets not previously published without official permission and, I would have thought, is aware of this obligation.

Many of us were nervous of what David Kahn would have to say when his turn came to review the book. When his review did appear in the *New York Review of Books*, it was surprisingly mild and harmless. He, of course, is in a different category. Not ever having been a part of

December 75 * CRYPTOLOG * Page 2

any Government agency, he cannot be regarded as subject to the same restrictions.

Other reviewers have been influential journalists who have taken the tone that the book has revealed the operations of World War II in a new light, that history will have to be rewritten, that the British have told only part of the story and that they will have to tell the rest. I do not know whether we have heard the last of this attitude.

Something has to be said about the paragraphs on page 14 of the book dealing with personalities. Winterbotham mentions the mathematicians Alexander, Babbage, Welchman, and Milner Barry, but doesn't seem to have heard of Turing, who is generally regarded as the leading genius of the methods of solution of the Enigma in its various forms. He says that "it was generally accepted that of our own backroom boys 'Dilly' Knox was the mastermind behind the Enigma affair." I do not agree with this at all, though I am aware that he was in general charge of the analysis of the machine before the war and long before the British had any success in solution. Incidentally, Winterbotham seems to confuse Knox with Foss, who fits much better into the physical description in the book and who had some influence on early solutions before

bombes became available. In his casual remarks about me, Winterbotham is somewhere near the truth: he says I had been borrowed from the Army. So I was -- 20 years earlier! Of Josh Cooper he says he was "another brilliant mathematician." Josh wasn't a mathematician at all -- he was a very fine linguist. For no known reason, Winterbotham mentions Dick Pritchard. He was a regular Army officer who had been with me for 8 or 9 years, before the war, but he had nothing whatever to do with the solution of the Enigma.

I think it quite likely that all this does no harm at all, but we cannot by any means be certain of this. Therefore, we have to continue to try to withhold further disclosures, particularly on technical methods of solution.

-(HVCCO)-

Brigadier Tiltman was Deputy Director and Chief Cryptographer, GCHQ, from 1941 to 1946. Since 1964 he has been working at NSA, Fort Meade. He is a Commander, Order of St. Michael and St. George; Commander, Order of the British Empire; and Distinguished Member, CMI.

ULTRA WAS SECRET WEAPON THAT HELPED DEFEAT NAZIS By P. W. Filby

(UNCLASSIFIED)

Shortly after the outbreak of World War II, the British Government acquired a stately home in a small town called Bletchley, a town renowned only for its railway junction and nearby brickyards.

For the next few months civilians and servicemen and women arrived in ever increasing numbers, and hardly a house in Bletchley escaped billeting. The citizens wondered at the motley crowd, raffishly dressed for the most part, often absent-minded and all having a studious air about them.

High iron fences were erected round the home known as Bletchley Park and armed Army guards were on duty at all times. The locals had to get used to comings and goings of their lodgers at all hours, and having taken in civilians they would suddenly see them emerge in full regalia as officers of the three services, especially when they made trips to London.

Many guesses were hazarded but the only thing that could be said was that it was a secret department -- and the secret was well kept, so well that it is not until now, thirty years later, that the Bletchley people and the world will know that the many thousands of people at the "Park" were working in enemy codes and ciphers. Group Captain Winterbotham has taken advantage of the "30-year rule" to describe the success of one group, "Hut 3." It is an absorbing story, and although the chief defect is that Winterbotham was not a codebreaker and therefore makes several wrong assertions, the book is one of outstanding interest, and readers will marvel at the war's greatest secret and how it was kept until now.

Just before the outbreak of World War II the British had obtained by various means a complex machine known as "Enigma" which was being used for the encoding of the most secret and important German armed forces communications. After a prodigious effort the British cryptographers of "Hut 3" managed to break this machine and later built what might well have been the first computer, so that the communications could be read immediately upon receipt.

To everyone's surprise, the Germans continued to use this machine throughout the war and thus most plans made by Hitler and his High Command were known to the British (and later, the Americans also) at the same time as the German recipients.

Radio operators in remote, lonely locations intercepted the messages, which were rushed to

December 75 * CRYPTOLOG * Page 3



Bletchley, often by motorcycle until more sophisticated methods were evolved, and were promptly decoded and passed to the appropriate commands. The intelligence was code-named "Ultra."

Astonishingly, there is nothing in captured German documents to suggest that anyone suspected that the most secret cypher code was being read throughout the war. Much of the credit for this were the rules laid down by Winterbotham for the "need to know."

For instance, the Russians were never told of it, and the many free forces (French, Dutch, etc.) were not let in on the secret. Winterbotham toured British and American commands, lecturing users on this intelligence and warning them care had to be taken on how the information could be used.

For instance, although the presence of an enemy force might be given in detail by Ultra, to bomb it immediately would cause the Germans to wonder how the enemy knew of this force, so reconnaissance planes had to be used so that the Germans would suspect that they had been spotted from the air.

Unhappily, it was not unusual for holders of the German plans to have to forgo using them for fear of compromising the cypher break. One such occasion was the bombing of poor Coventry; enemy plans were known beforehand, but to defend the city would have aroused German suspicions. Although attempts to defend were made, the populace was not warned in advance. At that time it was not known whether German spies were working among the British.

But the information was used with telling effect in the Battle of Britain, when the Air Force knew exactly the direction and the force to be employed in each attack. It is probable that Ultra did much to save Britain in those dark days. Everyone knew the Air Force could not withstand these onslaughts for long, but Ultra allowed them breathing space by parceling out the slender defense forces where needed most.

Ultra played a particularly distinguished part in the North African campaign, where Montgomery was informed of Rommel's disposition of his forces and the extent of his supplies. Ultra also enabled supplies across the Mediterranean Sea to be sunk en route. Montgomery's face should be red, since he claimed verbally and in his books that he planned his battle order, but he acquired the record of invincibility only through his use of the information given by Ultra.

With the British losing thousands of tons of shipping weekly, the decoding of the German Navy's messages provided a welcome respite, and from 1943 the losses were significantly reduced since the disposition of the U-boats was known.

One wonders now just how the Normandy landing would have worked out without Ultra. Since decoded messages told of the German belief that the attack would come from the narrow Pas de Calais, General Patton arrived with a phantom army to give the impression the landing would indeed be tried there. Consequently Rundstedt and a vast army were kept there, reducing the defenses in Normandy.

Ultra's strength was also shown when, in the Battle of the Bulge, the Germans relied on telephone rather than radio communications, and many lives were lost because the Allies could learn nothing of the German plans and intentions.

These and other exciting stories are related in this absorbing book. It suffers perhaps because Winterbotham was a "go-between" rather than one of the codebreakers, and thus credit is not given to the mathematicians and linguists who worked long hours in stuffy rooms where, because of blackout precautions, fresh air seldom penetrated the smoke-filled atmosphere.

Tribute must also have been paid to those radio operators, straining their ears when static and other conditions meant a missed group and maybe an important one at that, when the operator could not ask for a repeat -these were the real heroes of one of the <u>out</u>standing accomplishments of the war.

One amusing tailpiece to the whole affair is the effect it will have on those whose memoirs have already been written. Many should now be rewritten; if Ultra did not actually win the war it will cause historians to revise what has been written thus far. Books such as "D-Day" are exciting reading, but the present work must be included in all war history collections from now on, since it will affect all war histories in varying ways.

Winterbotham is rightly proud of Bletchley's achievement, but he tends to forget that information needs acting upon; it needs good generals and above all a great Air Force, Army, and Navy. Fortunately the Allies had these too, and though Ultra was one of the most important contributions to the victory, Winterbotham perhaps overrates it a little.

Sir John Masterman's book, "The Double-Cross System in the War of 1939-1945" (reviewed in these columns February 12, 1972) describes how captured spies were "turned around" and also contributed to the downfall of Germany. There were other great coups but Ultra and Double Cross must rank very high in the defeat of the Nazis.

> P. W. Filby, in addition to his SIGINT experience at Bletchley Park and GCHQ, is an "honorary NSA-er by marriage" (his wife is CLA President and CRYPTOLOG'S SRA Editor Vera R. Filby). Mr. Filby is the current Director of the Maryland Historial Society, Baltimore, Maryland. The preceding review is reprinted in entirety from the Baltimore Evening Sun, June 10, 1975. (FOUD)

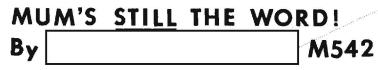
> > . .

,0,

1 -

December 75 * CRYPTOLOG * Page 4

UNCLASSIFIED



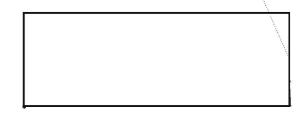
Many people make their work and the organization they work for an extension of their own egos, especially when the organization is performing a vital service to society. For most people, one of the most compelling motivations on the job is the quest for approval by their peers and supervisors. But we NSAers are not like "most people." True, we have always been able to rely on peer and supervisory approval, but we have never been able to derive ego gratification from identifying with NSA -- historically, both the Agency itself and our specific jobs here have been obscured from public notice. Lately, however, the curtain cloaking our activities has been lifted slightly. Winterbotham's book The Ultra Secret and the follow-on revelations in the CBS television program, "Sixty Minutes," have provided the public with glimpses of the vital role that cryptology plays in protecting our nation's security. Certainly, all of us must feel a sense of pride, and perhaps indulge our egos a bit, to see our Agency's vital function finally made known to the public. It's a very seductive thing. We plug along for years without public recognition. We strive constantly to overcome the natural urge to discuss our work with non-NSA friends, particularly when that work involves events taking place on the world stage. Then, suddenly, there's our organization, our work -- us! -- on the television screen, the front page of the newspaper, the public bookshelf. How easy it is to feel proud about finally getting public recognition. But that initial feeling of pride and personal gratification is soon outweighed by the disquieting realization that someone has talked, someone has betrayed our tradition of keeping our mouths shut.

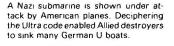
The fact that such revelations do not always compromise sensitive information, as in the case of *The Ultra Secret* and the TV follow-on, does not diminish our feelings of dismay. That precious shell of anonymity -- so carefully maintained over the years -- has been cracked. One can only expect that others will rush forth to give their versions of past events and open that crack still wider.



That our cryptologic operations are discussed at all in the public media, no matter how many decades have elapsed, is the primary concern here. Journalistic appetite begets appetite and, once titillated by the morsels served up by disclosures such as those in Winterbotham's book, it tends to become ravenous for the whole pot. Those who were associated with the cryptologic effort in the past -- and the numbers are prodigious -- as well as those currently involved, are presented with a psychological cop-out to indulge the r. Egos 6-300 talk about their work. After all, everyone else is doing it. Thus, revelation begets revelation.

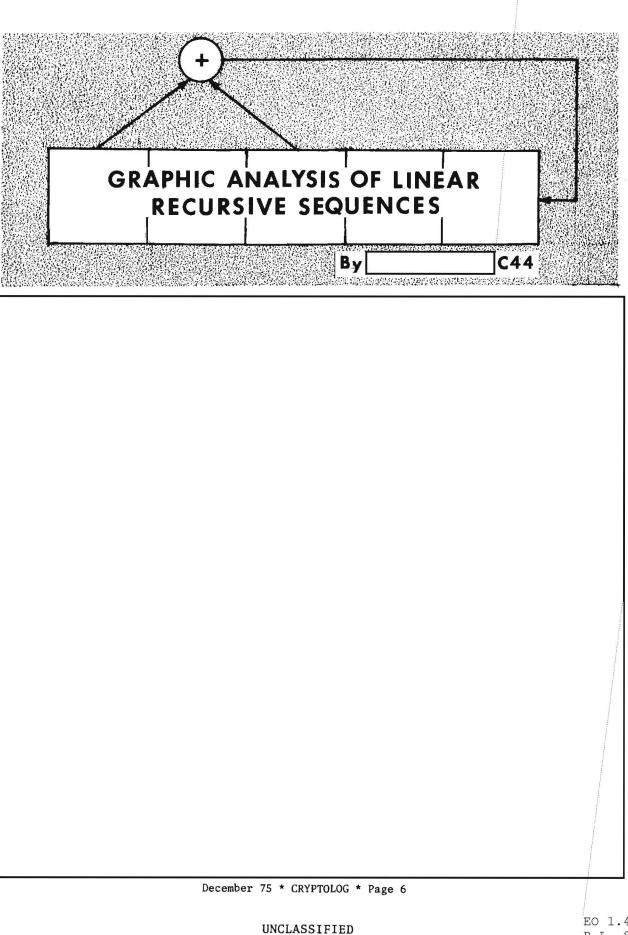
The publication of *The Ultra Secret*, however innocuous its specific revelations, can only be viewed with foreboding. It can only hasten the dropping of the next shoe. And when that shoe drops, we NSAers should remember, "Mum's *still* the word!"







December 75 * CRYPTOLOG * Page 5



EO 1.4.(c) P.L. 86-36

DOOID, ROOD/L/	DOCID:	4009727
----------------	--------	---------

C

December 75 * CRYPTOLOG * Page 7

UNCLASSIFIED

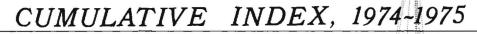
.

12 a a a a a

	1
We need your help in keeping CRYPTOLOG's distribution list up to date. Would you please fill in the attached form if you need:	
MORE COPIES? (New hires? people transferred in? somebody wants to be added to list?)	EO 1.4.(P.L. 86-
FEWER COPIES? (Resignations? retirements? transfers out? somebody wants off?) NAME CHANGES? (Misspellings on current distribution list? girls getting married and taking husband's name?	1121 00
guys getting married and adding wife's maiden name as hyphenated adjunct to his own?) ANY OTHER CHANGES?	
TO: Editor, CRYPTOLOG, P1	
Please make the following changes to distribution for: (Organization)	
ADD copies for:	
DELETE copies for:	
LABEL READS LABEL SHOULD READ	
(1f you do not want to cut this page, use plain piece of paper.) December 75 * CRYPTOLOG * Page 8	
Secondor 10 GATITOLOG Fage 6	
UNCLASSIFIED	

SECRET

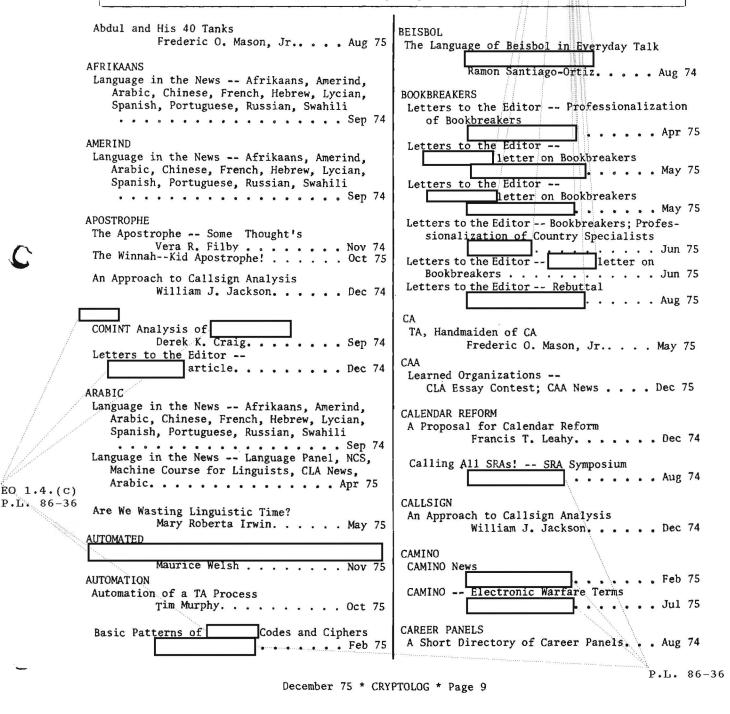
P.L. 86-36



The following cumulative index of CRYPTOLOG (Vols. I and II, 1974-1975), was computerproduced using the Super Bee CRT/Tycom typewriter terminal on the B6700 and programs written by George P. Wood, P16. The index is printed in the middle of this issue so that it can be removed and used as a separate document if desired.

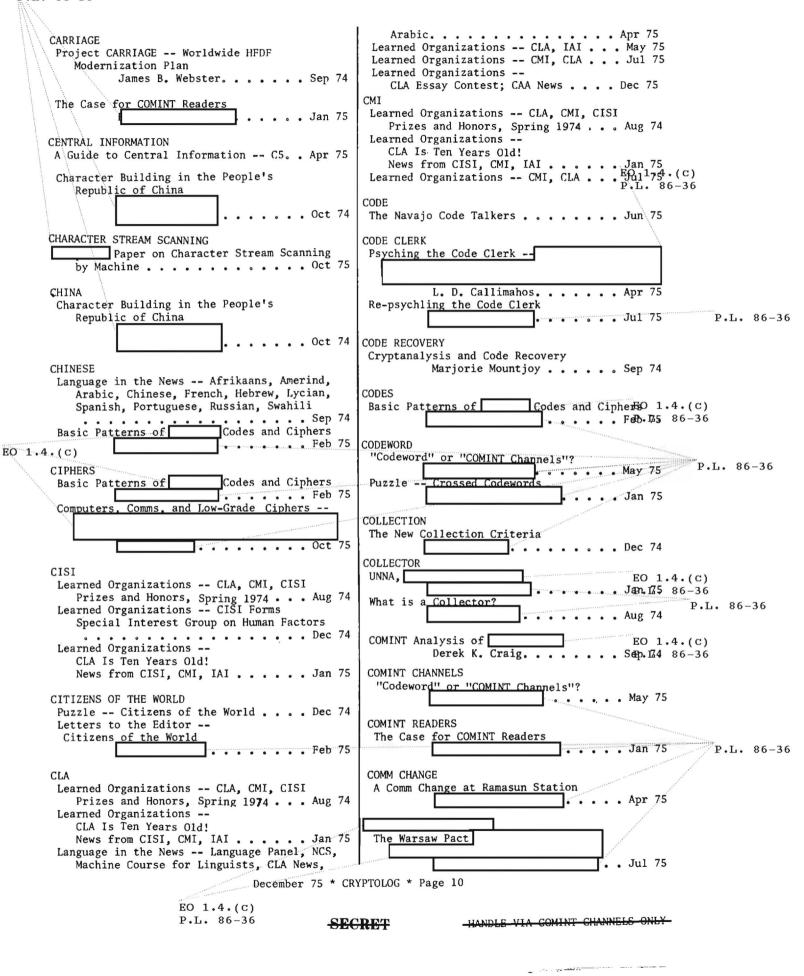
The index is in two parts. The first part is an index of <u>titles</u>, listed alphabetically (1) by title and (2) by keyword in the title. The second part is an index of <u>authors</u>. In both parts, multiple entries are listed in chronological sequence.

Items in the double issue February-March 1975 are indicated by "Feb 75," and those in the double issue August-September 1975 by "Aug 75."

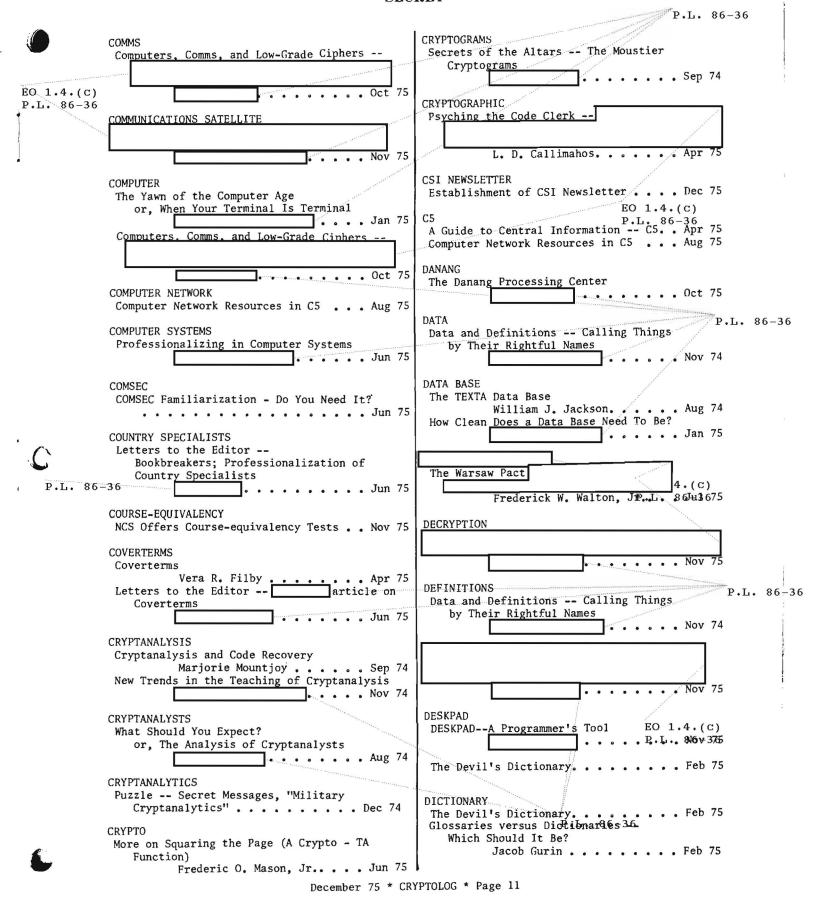


SECRET

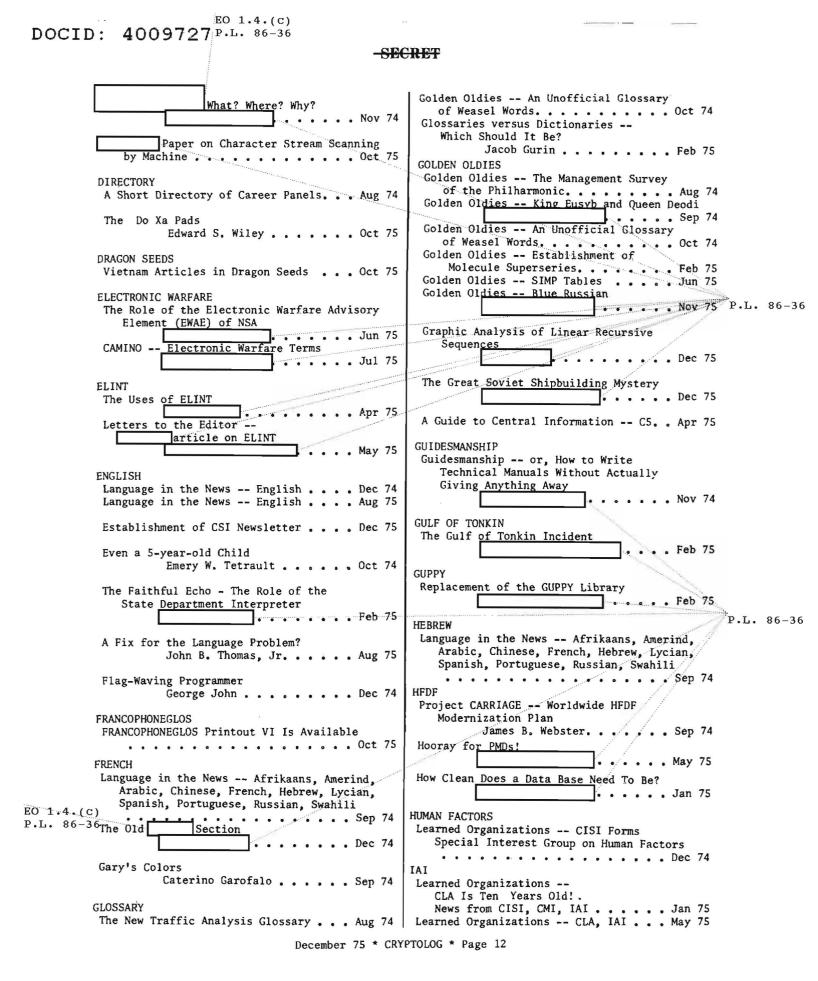
SECRET-



-SECRET



SECRET

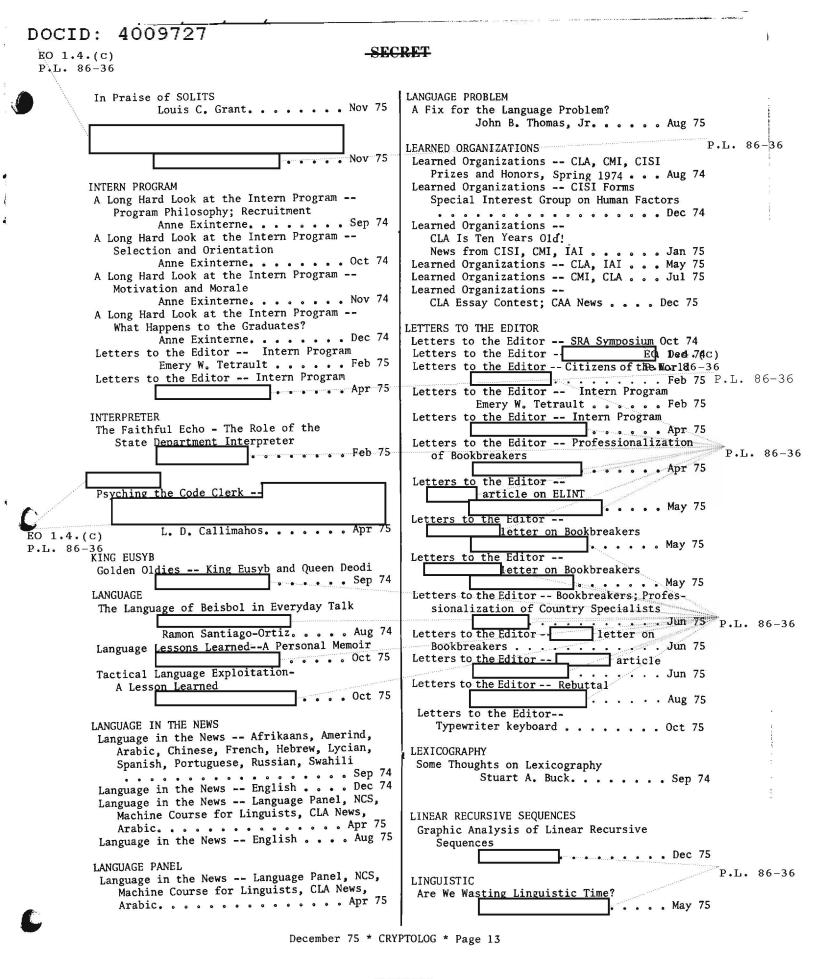


SECRET

- ·

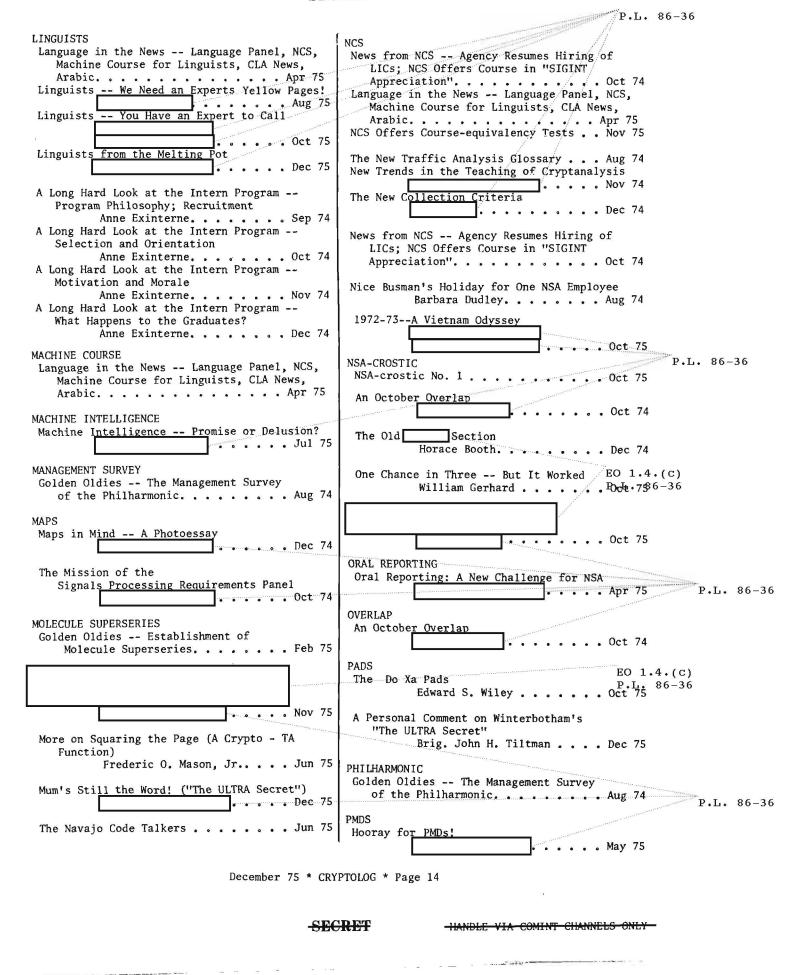
2 12

HANDLE VIA COMINT CHANNELS ONLY



SECRET

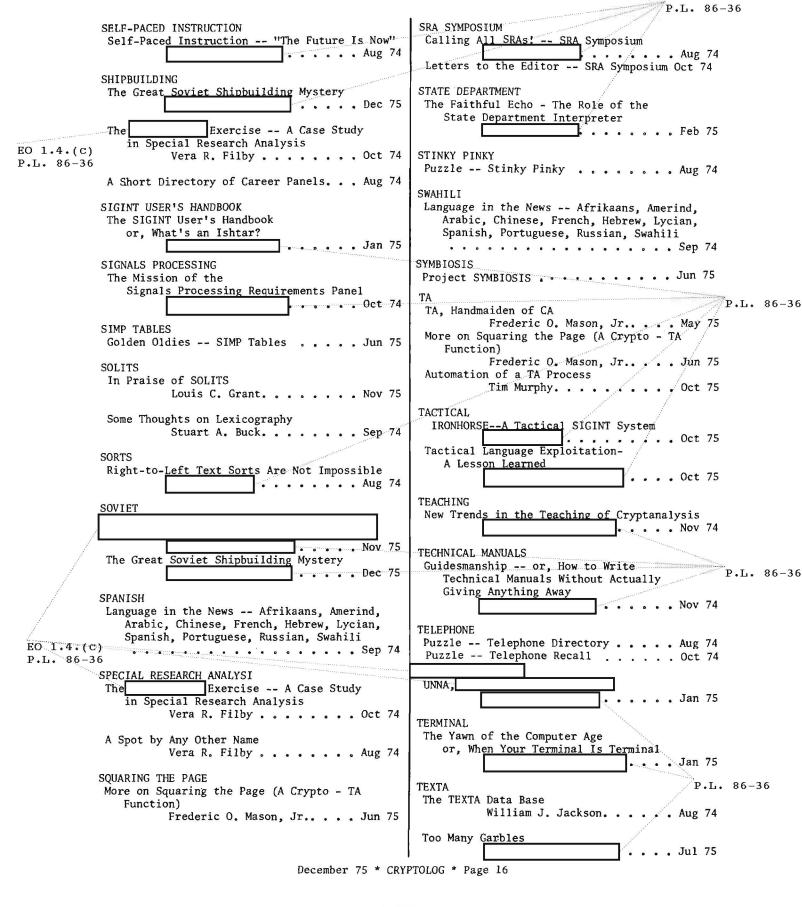
-SECRET



-SECRET

EO 1.4.(C) P.L. 86-36 Puzzle -- CRY-PTO-LOGrolling Aug 75 Puzzle -- NSA-crostic No. 1 Oct 75 PORTUGUESE Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, RADIOTELEPHONE Spanish, Portuguese, Russian, Swahili Puzzle --Radiotelephone · · · · · · · · · . Jun 75 PRIZES RAMASIIN Learned Organizations -- CLA, CMI, CISI A Comm Change at Ramasun Station Prizes and Honors, Spring 1974 . . . Aug 74 •••• Apr 75 Processing RANDOM Communications Typewriter Random -- A New Look EO 1.4.(C) ••••••• Aug 75 P. L. 86 Ad 9 75 PROFESSIONALIZATION RAPIDTRAN Letters to the Editor -- Professionalization RAPIDTRAN -of Bookbreakers •••• ••• • • Apr 75 Jul 75 Letters to the Editor --Bookbreakers; Professionalization of Reflections on a Translators' Conference Country Specialists •••• Nov 74 •••• ••••• Jun 75 Replacement of the GUPPY Library PROFESSIONALIZING •••• Feb 75 Professionalizing in Computer Systems Re-psychling the Code Clerk Jun 75 Jul 75 PROGRAMMER Flag-Waving Programmer REVIEW P.L. 86-36 George John Dec 74 Review of "Guide to Russian Technical" DESKPAD--A Programmer's Tool Translation." by Arthur J. Salemme •••••••• Nov 75 •••• Feb 75 Project CARRIAGE -- Worldwide HFDF RIGHT-TO-LEFT TEXT Modernization Plan Right-to-Left Text Sorts Are Not Impossible James B. Webster. Sep 74 ••••••••••••••• Aug 74 Project SYMBIOSIS Anonymous Jun 75 The Role of the Electronic Warfare Advisory Element (EWAE) of NSA A Proposal for Calendar Reform ••••••• Jun 75 Francis T. Leahy. Dec 74 RUSSIAN Psyching the Code Clerk --Language in the News -- Afrikaans, Amerind, Arabic, Chinese, French, Hebrew, Lycian, Spanish, Portuguese, Russian, Swahili L. D. Callimahos. Apr 75 Purity of the Russian Language --Purity of the Russian Language --P.L. 86-36 Slavophiles vs Westernizers Slavophiles vs. Westernizers • • • Nov 74 . . . Nov 74 Review of "Guide to Russian Technical Translation," by Arthur J. Salemme PUZZLE Feb 75 Puzzle -- Stinky Pinky Aug 74 Puzzle -- Telephone Directory Aug 74 P.L. 86-36 Puzzle -- Telephone Recall Oct 74 Golden Oldies -- Blue Russian Puzzle -- Secret Messages, "Military •••••• Nov 75 Puzzle -- Citizens of the World Dec 74 Puzzle -- Crossed Codewords Processing Jan 75 Communications Puzzle -- Can You Make Out the Name? Aug 75 Feb 75 Puzzle -- How Many Words in "CRYPTOLOG"? Secrets of the Altars -- The Moustier Puzzle -- Radiotelephone . May 75 Cryptograms ••••••• Sep 74 • • • • • • Jun 75 December 75 * CRYPTOLOG * Page 15 P.L. 86-36 EO 1.4.(C) SECRET HANDLE VIA COMINT CHANNELS ONLY P.L. 86-36

SECRET

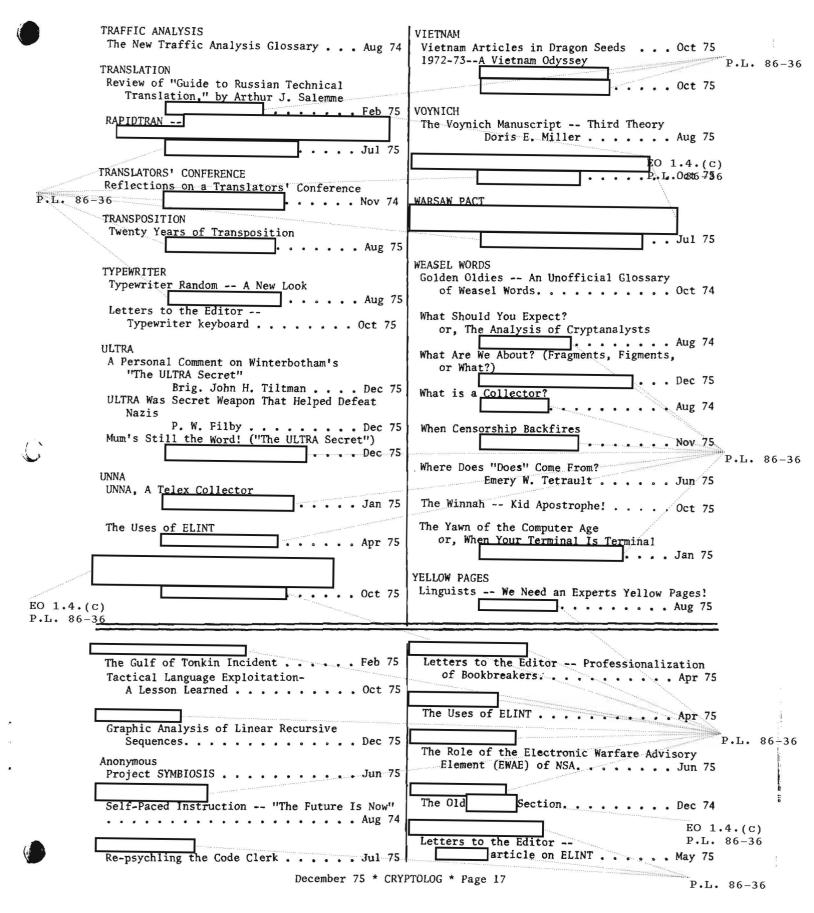


SECRET

مستعادة والمستعدة منشية والمستعدية المستجد فتوار والمستجد

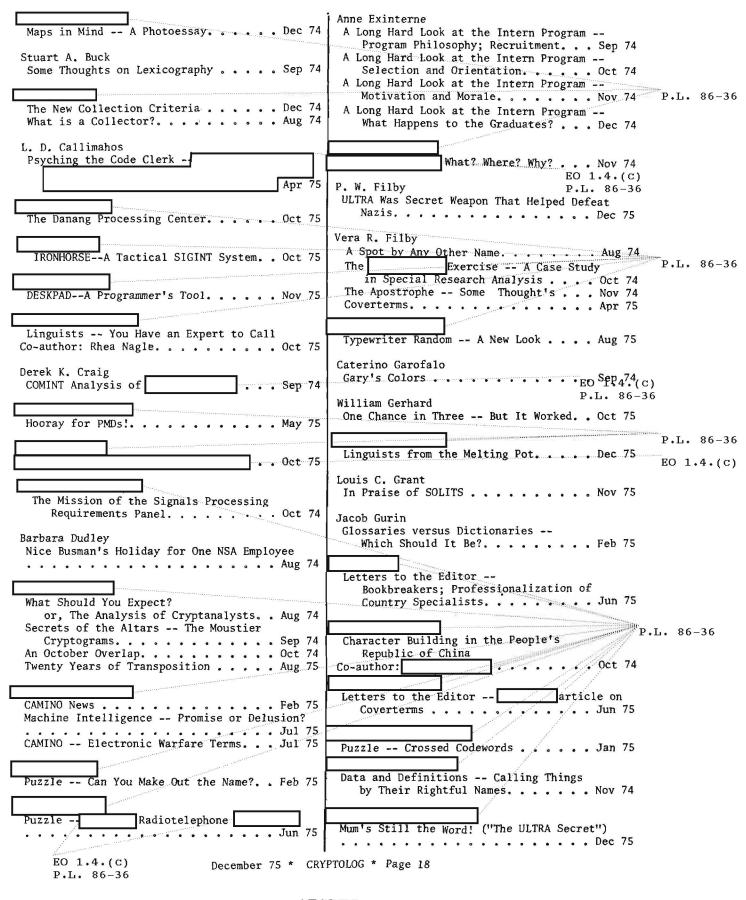
Martine Inc.

SECRET



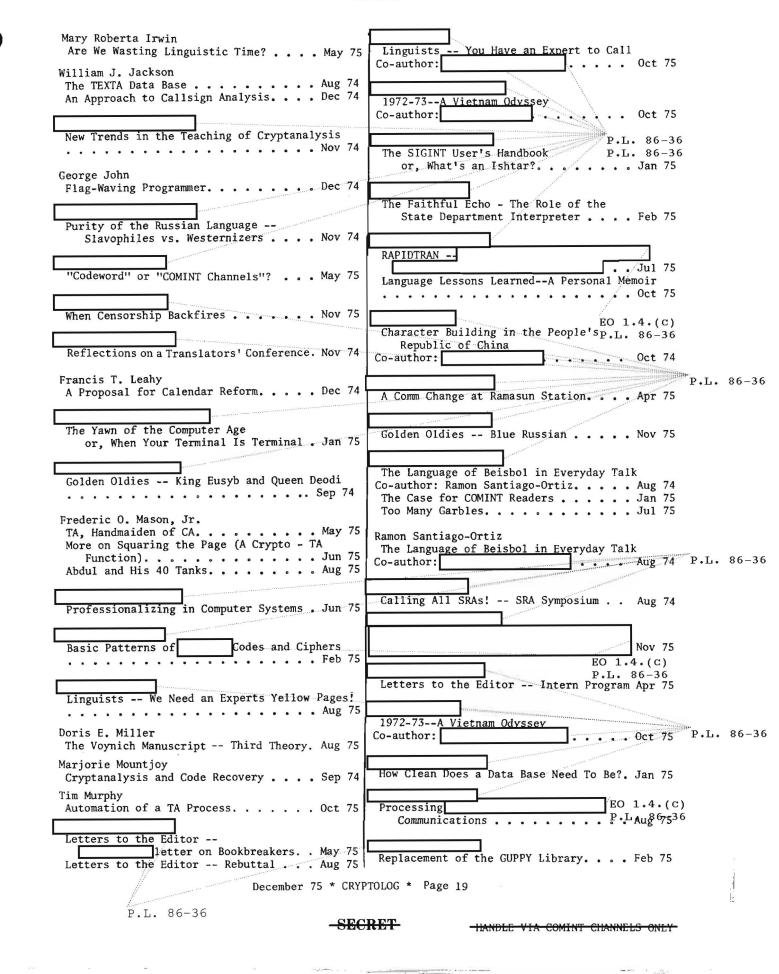
SECRET

SECRET

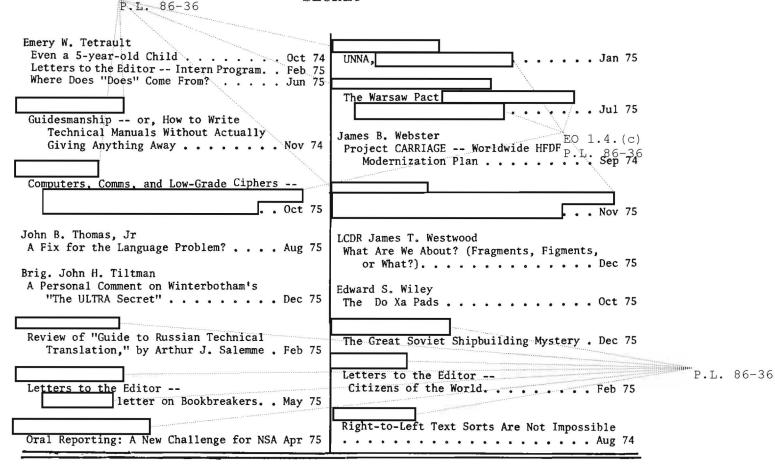


SECRET

SECRET

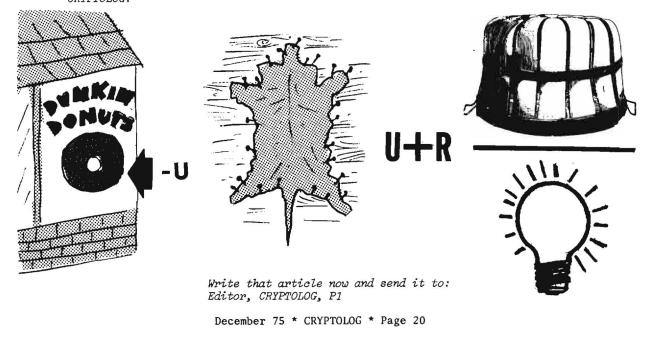


SECRET



CRUPTOLOG Rebus

If your name is not included in the list of authors' names, and you have an idea for an article about a subject that hasn't been dealt with yet in CRYPTOLOG:

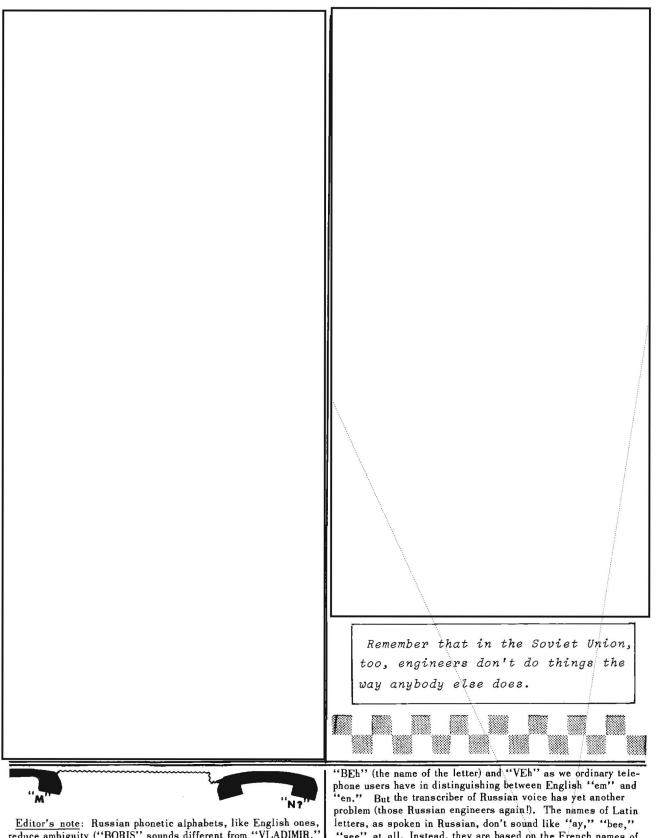


-SECRET



December 75 * CRYPTOLOG * Page 21

TOP SECRET UMBRA



reduce ambiguity ("BORIS" sounds different from "VLADIMIR," just as "Mary" sounds different from "Nancy"). Since phonetic alphabets are not used universally, transcribers of Russian voice often have as much trouble distinguishing between

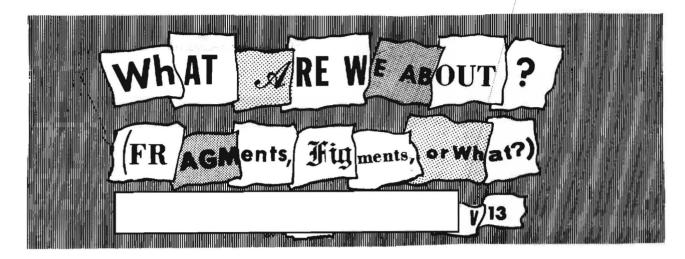
"see" at all. Instead, they are based on the French names of the letters. Hence, Latin H, as pronounced by a Russian engi-neer, is not like the English "aitch," but is "ASh" (French "ache"); Y is not "wye," but "IGREK" (French "y grec").

December 75 * CRYPTOLOG * Page 22

EO 1.4.(c) P.L. 86-36

TOP SECRET UMBRA

SECRET



The collection and dissemination of defense intelligence, or any other kind of intelligence, does not have to be especially complicated, so long as certain fundamental principles and goals are kept in mind. Defense intelligence, in which NSA/CSS and the Service Cryptologic Services are heavily involved, should seek to answer certain elemental questions in peacetime, wartime, or several other somewhat nebulous "times" between peace and war. These questions include:

- Do we have an enemy/adversary? If we do, who is he and why is he an opponent?
- Where is he and in what strength?
- What are his intentions?
- What are his perceptions of himself, his own purposes and goals?
- Are his intentions consistent with his strength (capability)? If not, might he be practicing deception?

Within defense intelligence, the business of signals intelligence is to "read the enemy's mail." This assumes that there is a bona fide enemy. Given the U.S. national interests, reading the enemy's mail requires a massive effort. For one thing, it takes a vast amount of mail to yield real nuggets of value on a continuing basis. It follows that, if the processing and reporting effort ever catches up with the collection effort, we would be in real trouble because we would certainly have the cart before the horse. There is, however, a sometimes overlooked proviso in this relationship: Any major SIGINT effort whose thrust is not in line with reading the enemy's mail (in an admittedly broad sense) is probably superfluous and ought to be redirected or abolished, because resources are limited and we must, therefore, keep expenditures of those resources tied to our fundamental purposes.

Of course, "reading the mail" is a figurative phrase. It does not mean just CA and TA. It means all that we do with men and machines that allows SIGINT to work its effectiveness in terms of timeliness, uniqueness, and fidelity, that is, the faithful reflection of the enemy's intentions and activities.

Intelligence, in whatever form and from whatever source, is a service provided to decisionmakers. Decision-makers are civilian and military officials with distinct responsibility and personal accountability for solving problems that affect the public welfare. To make effective deployment of the people and property constituting their responsibility, the decisionmakers need certain information, much of which we have come to call intelligence. But this intelligence is not an end in itself. It does not exist to promote and serve itself. It exists to give decision-makers the best it can provide in the way of current, accurate, reliable information to answer the vital questions they have to answer. Additionally, and by its very nature, intelligence must be anonymous and quiet. A secret is best kept by not revealing it. Mr. Colby was recently quoted as saying, "Intelligence. . .will not work if exposed."

There is no small amount of confusion and resultant ineffectiveness at large in the intelligence business today because of the tendency of intelligence producers to provide intelligence users with too much, too fast, too often -that is, because of the "shotgun" approach. This tendency results from our attempt to cover ourselves against the possibility that we might fail to tell somebody something that he really needs to know. Morever, because we collect a lot of intelligence, we feel compelled to process a lot. That leads to wanting to report a lot, and, in turn, to inundating the user with so much intelligence that he cannot give certain portions of it the necessary attention. This gives rise to certain attendant problems: This tendency to broadfire intelligence then leads to the tendency for intelligence producers to dictate, however subtly or indirectly, how much of what kind of intelligence the users shall receive and, moreover, in what format and at

December 75 * CRYPTOLOG * Page 23

SECRET

-SECRET

what rate they shall receive it. These tendencies are especially visible in terms of SIGINT support to military commanders. The result in this instance is that we make military commanders passive recipients of intelligence. An active role, with commanders saying, "This is what I want to know and this is how much I want," is precluded by a deluge of "This is what we want you to have." If this is drawn out to its ultimate conclusion, the presumed goal of "increased accessibility to intelligence product by decision-makers at all levels" is unattainable.

Those who pay close attention to dissemination might disclaim the existence of these tendencies. They might attempt to explain the present situation by splitting intelligence into "tactical" and "strategic." But the difference between "tactical" and "strategic," to my mind, lies not so much in the nature and content of the intelligence itself, as in the level or scope of the decision-making that the intelligence is supposed to serve. For example, was it tactical or was it strategic intelligence which foretold the Chinese crossing of the Yalu River into Korea? Obviously, it was both: it was tactically useful intelligence to the field commanders in Korea, and it was also strategically useful intelligence to the President and his Cabinet. We do our SIGINT profession an immense disservice when we fragment our efforts and our product into pieces and parts in an attempt to serve two or more users, for example, the tactical commander and the national decision-maker.

Perhaps we should devote some time away from the production process in order to get from all our users a clearer idea of what they would consider to be useful. Intelligence production today is much more efficient than ever before, given our increasing reliance on automatic data processing. Whether it is also effective is another question. Effectiveness is the accomplishment of objectives -- the satisfaction of requirements. Machines are not a substitute for human judgment. Decision-makers want to know that human judgment has been brought to bear to weigh the significance of the intelligence that is being machine-processed so efficiently for them.

Tactically, the fundamental questions have not changed since Moses sent spies into the Land of Canaan: Where is the enemy and in what strength? Strategically, basic questions persist: What are our interests and what and how much do we need to know about threats to those interests?

What are we about, then? We are about the business of providing intelligence service to decision-makers. We ourselves are not those decision-makers and we must resist the tendency to confuse roles. It is not in the nature of our business to decide what is strategic and what is tactical. We have skills and facilities that can respond to intelligence needs at various levels, often simultaneously, but not by saturation.

SIGINT is part of a larger intelligence business which, itself, requires us intelligence producers to integrate our efforts and to tailor our production and dissemination to answer the fundamental, but related, questions posed by a variety of users. Those users can best be served from the same, single set of resources if we all appreciate what we are about.



NSA COMPUTER SYSTEMS INTERN PROGRAM

The Intern Panel Advisory Board (IPAB) has established a new monthly publication, the *Computer Systems Intern Newsletter*, in order to provide "lines of communication both to and from the Interns themselves" and "to better inform and advise those associated with the Computer Systems Intern Program." The publication is classified FOR OFFICIAL USE ONLY and began with the September 1975 issue.

Anyone who would like to receive back issues or to be put on the distribution list should contact the Editor, R214, 3460s (FOUO).

December 75 * CRYPTOLOG * Page 24

D	.L.	86-	21
P	1000	8 n-	- 3r
-		00	00

-SECRET

Bv

UNCLASSIFIED

LINGUISTS FROM THE MELTING POT



P.L. 86-36

For several years, NSAers who grade language hiring examinations have noted that people's names do not always match up with their expected language ability: an applicant named, say, Yamashita can score horrendously on the Japanese hiring examination, and someone named Olivetti can do just as badly on the Italian. But it is often difficult to convince managers commissioned to "solve the language problem" that the solution to, say, the "Russian language problem" is not just a matter of running out and hiring 100 American citizens with names like Ivanov and Fedorenko. The following article by (NSA retiree), which is

reprinted from *Keyword* (November 1971), deals with some of the reasons why Americans with foreign surnames often show a surprising lack of knowledge about the language they supposedly picked up at their mother's or grandmother's knee.

It is a common belief that since a large part of the United States population is made up of immigrants and the children of immigrants there is a ready source of foreign-language talent for any emergency. To a degree this is true, but the source has many limitations. Any language must undergo changes if its speakers are moved to a strange environment, and the speech of the immigrants to the United States is no exception.

If you examine the "Help Wanted" section of the German-American press, for example, you will find a large number of English words used to designate skills or crafts. At first there seems to be no pattern in the choice of German or English words, but the existence of Backergeselle (journeyman baker) in one advertisement not far from another that seeks an erstklassigen body-and-fender-Mann (first-class body and fender man) suggests that the borrowings are in response to a world of labor in which there is a greater, or perhaps only different, specialization. For the unfamiliar specialty the immigrant has a choice of coining a new word in his own language, or simply of borrowing directly from the other language. There are still other means of meeting the problem.

The book I Trapiantati (The Transplanted), written by Giuseppe Prezzolini, an Italian foreign correspondent in New York, and published by Longanesi & Co., Milano, 1963, contains two chapters dealing with this subject as it concerns Italian-Americans. Since the general situation presented may be considered typical of many immigrant groups, I have gisted them briefly below.

Italians who visit the United States and come in contact with others who have settled here for one or two generations are amazed, puzzled, and sometimes horrified at the language they hear used by those who, like them, call themselves Italians. It is the same impression as that received by visitors, journalists, and consular employees who came here in decades past. What they heard was not Italian, it was not dialect, nor was it even English; still it was at the same time a little Italian, a little dialect (and this varied from place to place and sometimes from person to person), but it regularly revealed an English-language base, pronounced in the Italian fashion, that is to say an English root, with the round, vowel endings of Italian. For example there was:

contrattore	contractor
la tracca	track
la grosseria	grocery
il bordante	boarder

Their amazement increased when they found this jargon written (often only approximately) in restaurant menus, the classified ads of Italian-American newspapers, and even in official documents of American authorities who wanted to be understood by Italian immigrants. "American Italian" was a *deformation of English* rather than an adaptation of Italian. It was the result of the effort made by a mass of poor and ignorant country people, dependent upon employers who spoke a foreign language, to make themselves understood by the latter and by their own fellow workers.

Anthony Turano, an American writer of Italian origin, observed very correctly that the rural origin of most immigrants made a mechanical vocabulary difficult for them. To express their needs the southern Italian peasants were compelled to use English terms, since they had never known the Italian equivalents. But in adopting the English terms they transformed them, as best they could, by making them phonetically similar to Italian. Turano distinguished three categories of borrowings:

December 75 * CRYPTOLOG * Page 25

UNCLASSIFIED

P.L. 86-36

. words remote from the immigrant's former life:

sexa, sescia	(railroad) section
rancio	ranch
rodomastro	roadmaster

words for things unknown to him before he came to America:

fensa	fence	
morgheggio	mortgage	

words that stuck in the immigrant's mind by dint of constant repetition, even though he knew the corresponding Italian words:

stritto	street
denso	dance
carro	car

There is also a well-known linguistic phenomenon by which a people when it accepts a foreign word finds one in its own language which is similar to it and which it adapts to the new use even though it may have a completely different meaning. For example,

sciabola	(saber)	shovel ¹
olivetta	(kind of sausage)	elevator, elevated
	(tuna fish)	tunnel

At times the marriage of English and Italian involves a dialect, as in the case of coppastese (Neapolitan 'ncuop + English stairs), upstairs; or coppetane ('ncuop + English town), uptown. The Sicilians, however, do not use this expression, but instead say oppitauni.

In making a list of words in the American Italian jargon, it is easy to see that the proportion of adjectives to nouns is very small -- much smaller than in either Italian or English. The immigrant had to be able to express $pezze^2$ (dollars), or bosso (boss), but not necessarily "pretty" or "good" or "true" or "false." Orre! (Hurray!), an expression from the American-Italian variety shows, barely reveals a feeling of admiration, and naise (nice) a favorable opinion.

At first, newspapers in the Italian language adhered fairly closely to standard Italian, but after about 1900 the flood of classified advertisements made it impossible to conceal or trans-

¹Another observer mentioned his amazement at being told by an immigrant countryman that there was plenty of work in the United States for a man who knew how to use picca e sciabola, which in Italian means "pike and saber," but in American Italian, "pick and shovel." (R.E.G.)

²Pezze may be used because of Spanish peso. The word was commonly used in Nevada in a rudimentary Spanish-Italian jargon used by immigrant laborers of both nationalities when working together. Scudi and dollari were used by other Italian speakers, as I recall. (R.E.G.)

late the jargon of the Italian-American working man. In the Bolletino della Sera in 1917, advertisements are found for:

sceperi	shapers (of garments)
pressatori	pressers
sottopressatori	pressers' helpers

There were also to be seen advertisements for a mezzo-barista (a man to work half a day in a bar). In these pages a country place was always a farma (farm). Heating was done with stima (steam, but meaning in Italian esteem), and a frequent advertisement was for sale of a casa senza stima -- a house without heat or without esteem, depending on how well you understood American English.

This occurs less and less frequently. Such expressions have almost disappeared from the classified advertisements of Il Progresso Italo-Americano, not because the older generation doesn't still use them, but because that generation no longer has to work. The new generation of Italians who are looking for work know Italian pretty well and do not need the job opportunities translated into jargon. Nobody is trying to buy a fruttistenne (fruit stand) any more.

Prezzolini feels that the whole of this interlingua will probably have ceased to exist within a few generations. since the more recent immigrants (much fewer in number) arrive under quite different circumstances. In Italy they have learned the logical bases of the Italian language (it must be remembered that a large part of the older immigration was illiterate) and here, as soon as they go to school -- even the adults -- they learn English and are (quoting Prezzolini) the first to be horrified at the crude linguistic mixture of their predecessors. Undoubtedly, the language he describes will vanish since it was based on the southern dialects of Italian and was the hasty creation of peasants abruptly thrust into an urban world. The newer immigrants more frequently speak standard Italian and are literate, often cultured people. So long as their Italian is a tool used in a foreign society, though, it must adapt, and it will evolve into an American Italian much different from the parent language.

With some exceptions, the immigrants of any nationality are much more concerned with earning a living, raising a family, buying a car, or any of a host of other things than they are in preserving the purity of their native languages. Their children will necessarily speak a truncated language, adequate for the needs of the family or neighborhood, but shot through with words borrowed or transformed from English. The value of the family-trained linguist to SIGINT should not be underestimated because of these limitations, but at the same time it should be recognized that this source produces only raw material that must be trained and developed.

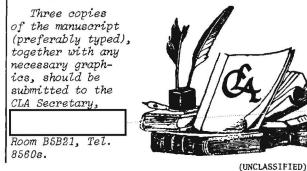
December 75 * CRYPTOLOG * Page 26

-CONFIDENTIAL

CLA ESSAY CONTEST

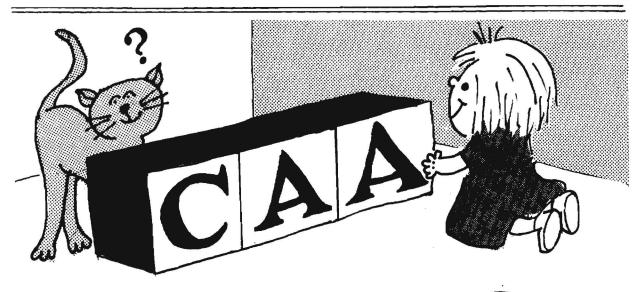
The tenth annual essay contest of the Crypto-Linguistic Association is now open. Papers will be accepted until 19 March 1976. A panel of three judges will select the three best, which will be awarded prizes of \$100, \$50, and \$25 at the CLA's spring meeting. Every entry will be considered for publication in whichever of the Agency publications is most appropriate for its content and style.

The purpose of the contest is to encourage writing on topics concerning application of linguistic knowledge to the solution of Agencyrelated problems. Any writing on cryptology or a significantly related topic may be entered. Papers may be classified up to TOP SECRET CODE- WORD. Any NSA or SCA employee (CLA member or nonmember) and any nonemployee CLA member may enter the contest.



P.L. 86-36

.....



CAA-What's that?

"That" is the Communications Analysis Association, one of the Agency's Learned Organizations. The CAA was established in 1968 "to promote increased professionalism in the career fields of Traffic Analysis and SIGINT Research" by encouraging professional contact among its members and specialists in related fields; by conducting workshops and lectures; by encouraging the writing of technical papers to document the disciplines; and by recognizing those who advance the art and science of traffic analysis and SIGINT research. Membership in the CAA was originally restricted to professionals and aspirants in TA and SR in the U.S. Cryptologic family and collaborating agencies, but it was later opened to those in the related fields of Signals Collection, Signals Analysis, Cryptanalysis, etc. At one time the Association published the technical magazine COMMAND, now incorporated into CRYPTOLOG.

So far this 1975-1976 lecture year, the CAA has sponsored the following lectures:

- "GUARDRAIL" (Col. Norman Campbell),
- "Changing Emphasis in the USAFSS"
 - (Maj. Gen. H. P. Smith), and
- "SIGINT in Vietnam: Lessons Unlearned"

All three lectures drew standing-room-only audiences of members and nonmembers to the Friedman Auditorium. The Association, under its President, Frank Smead, is outlining a program of lectures and other activities for 1976 which will be in keeping with the organization's stated objectives.

Anyone interested in joining the CAA should call its Treasurer, Tim Murphy, on 4787s or its Secretary, Jane Dunn, on 8025s for more information.

-(CONFIDENTIAL)-

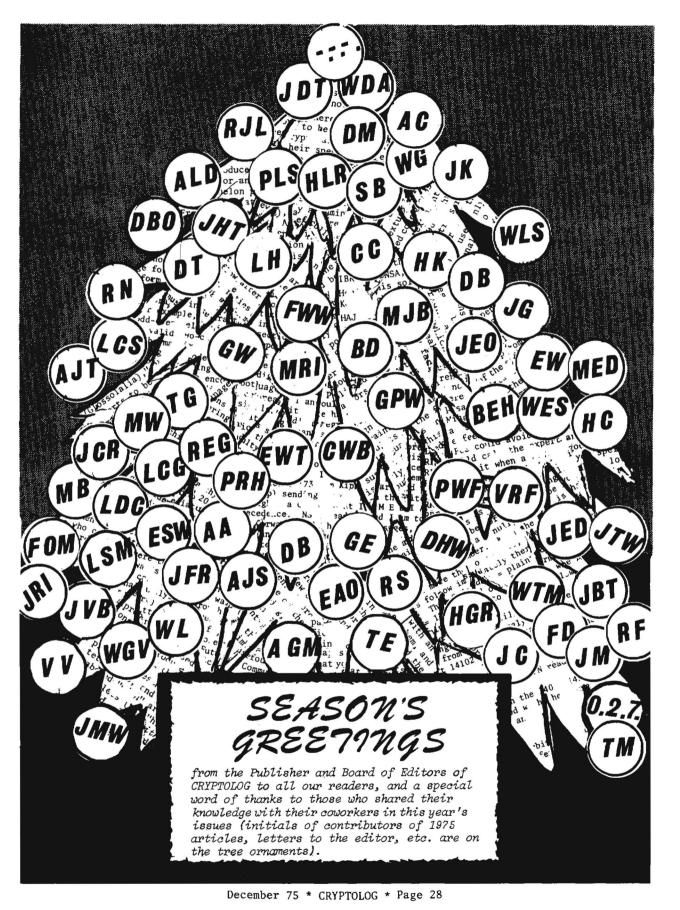
December 75 * CRYPTOLOG * Page 27

- CONFIDENTIAL

1.11

P.L. 86-36

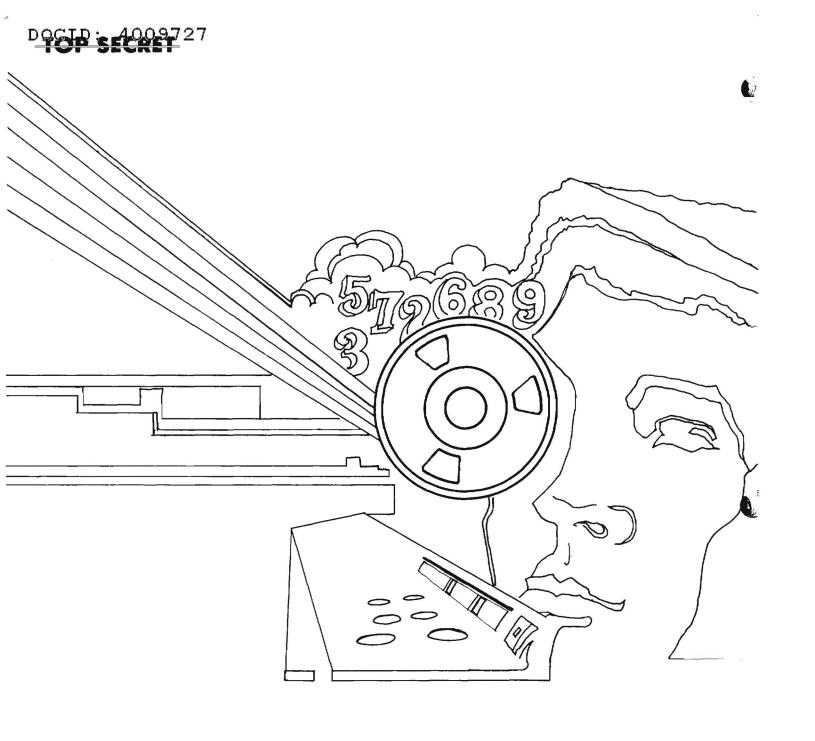
UNCLASSIFIED



1.7700. N. YI

UNCLASSIFIED

P1-Nov 75-S3-24264



<u>____</u>

-THIS DOCUMENT CONTAINS CODEWORD MATERIAL

TOP SECRET