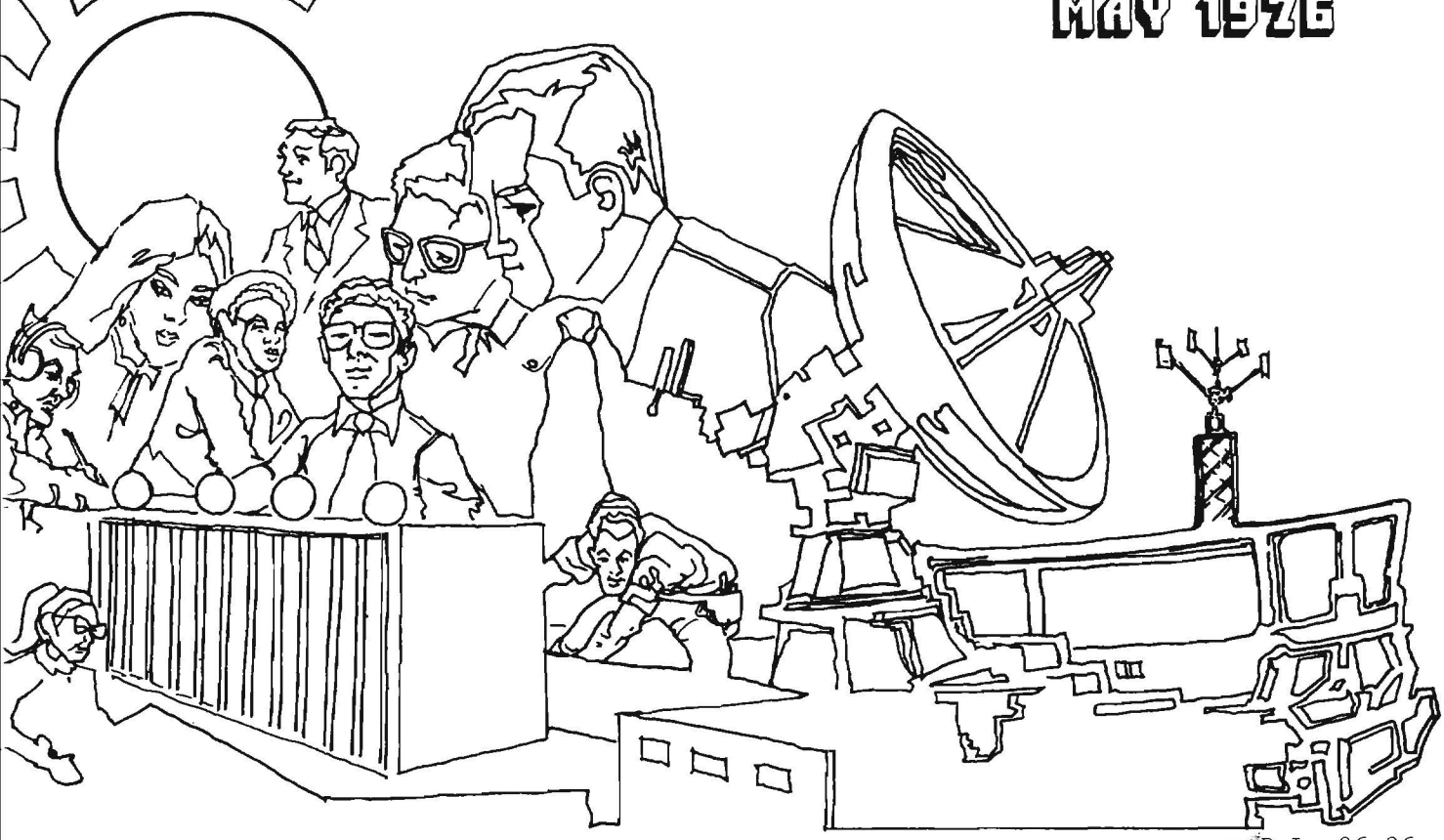
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1976



P.L. 86-36

~~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~~

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

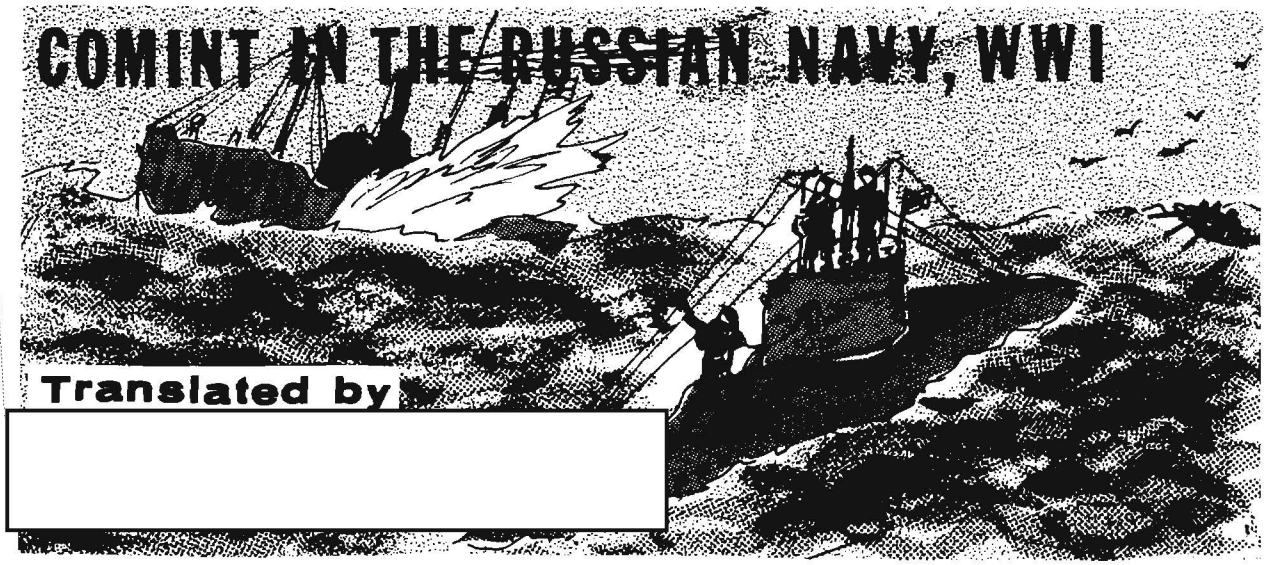
VOL. III, No. 5 MAY 1976

PUBLISHER WILLIAM LUTWINIAK

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

COMINT IN THE RUSSIAN NAVY, WWI



Translated by

[redacted]

Translator's note: *The following article is a translation of "On the Origins of Communications Intelligence in the Russian Navy," by V. Yankovich, in the Soviet periodical* Voenno-Istoricheskij Zhurnal (*Journal of Military History*), *February 1961, pp. 114-117. In my search of open-source materials, Yankovich's article was the only one that I could find that describes the early development of the Soviet signal intelligence service from the point of view of a participant. The article does not contain any attribution as to the source of the information, or any identification of the author except by name. Because of the article's unique nature and its interest to CRYPTOLOG readers, I have translated it in its entirety.*

At the beginning of World War I not one of the combatant sides had a specially organized communications intelligence (COMINT) service [*radiorazvedka*] in its navy. The first steps toward organizing a COMINT effort in the Russian Navy were, to a large degree, connected with the wreck of the German cruiser Magdeburg near Odensholm Island on 26 August 1914. Documents discovered on that ship revealed a system of enciphered radio communications that the enemy had been using at that time[1].

After Germany declared war on Russia on 1 August, the enemy fleet in the Baltic Sea limited itself for a prolonged period of time to demonstrations carried out by small forces and the patrol service in areas of possible Russian naval action.

In the early hours of 26 August the Russian patrol cruisers Pallada and Bogatyr' were standing at anchor in Baltijskij Port (now Paldiski) because of fog. At 0130 hours the signal station on Odensholm (now Osmussar) Island reported by telephone to the Chief of the Signal Service in Revel (now Tallin) that a ship had run aground at a distance of two cable lengths from the island. Then the signalmen reported that they could hear German being spoken and the operation of shipboard machinery, and could also hear the anchors being veered and heavy objects being thrown overboard. When the fog lifted somewhat, the signal station reported that a four-funneled cruiser had run aground and that a torpedo boat was standing by it, attempting the tow the cruiser by the stern. Upon receiving the very first report in Revel concerning the accident that had befallen the German ship, the Fleet Commander dispatched the First Torpedo Boat Division and the cruisers Bogatyr' and Pallada to Odensholm Island. The chief of the fleet communications service set out to sea from Revel on board the torpedo boat Lejtenant Burakov, accompanied by the torpedo boat R'yanyj; they were followed somewhat later by the cruisers Rossiya and Oleg, and, finally, the Ryurik, under the flag of the Fleet Commander.

The cruisers Bogatyr' and Pallada approached Odensholm in the fog and, at approximately 1100 hours, when the visibility had temporarily improved, they spotted the German cruiser Magdeburg aground, with a tow line from the large German torpedo boat, the V-26, attached to its stern. Our cruisers opened fire on them. The

[1]It should be noted that the descriptions accompanying the charts in *Morskoj Atlas* (Naval Atlas) (Vol. 3, Part I, Publishing House of the Main Staff of the Navy, 1959, p. 769) and in *Istoriya Voenno-Morskogo Iskusstva* (History of the Naval Art) (Vol. 3, Moscow, Voenizdat, 1953, p. 120) are not completely accurate in illuminating the circumstances under which the documents were found on the German cruiser Magdeburg, or about their contents. (Author's note)

Magdeburg responded, but its situation was hopeless, and, as was subsequently reported by captured German sailors, the commander decided to blow up the cruiser. The V-26 was ordered to approach the Magdeburg and take off the crew. However, it failed to throw out the mooring lines. Taking advantage of the dense fog, the torpedo boat left. After it departed, the forward magazines of the Magdeburg were exploded.

When visibility improved, it became clear that the Germans had abandoned the cruiser. The Lejtenant Burakov approached the Magdeburg. The only people remaining on it were the commander and two sailors. Approximately 50 crew members were found on the island and in a lifeboat. They were taken prisoner.

A large number of bundles and suitcases containing personal articles belonging to the cruiser's crew members were transferred from the Magdeburg to the Lejtenant Burakov. The articles included notebooks and diaries. A signal book was found in one of the bundles. The discovery of the signal book was reported by semaphore to the cruiser Ryurik, which had also approached Odensholm at that time.

The fleet Chief of Staff, together with several officers, including myself -- at that time I was a staff flag officer -- set off from the Ryurik on board the destroyer Pogranichnik to inspect the Magdeburg. When inspecting the radio room, I noticed under a desk a cardboard folder containing a piece of paper with penciled notations. The notations might have been of interest, so I took the folder with me. That insignificant little piece of paper turned out to be a very valuable document.

Upon the Ryurik's return to the Revel roadstead, the Chief of Staff ordered me, as a person with a good knowledge of German, to acquaint myself with the captured materials and to report the results to him. After setting down to work, I noticed that the authors of most of the diaries and notebooks dwelt especially on the events of 17 August.

On that day (17 August 1914) a brigade of Russian cruisers consisting of the Gromoboy, the Admiral Makarov, the Pallada, and the Bayan, under the command of Rear Admiral Kolomejtsev, was on patrol on the meridian of the Pakerort (now Pakkineem) lighthouse. At approximately 1500 hours, our observers noticed smoke to the west of Takhkon (now Takhkuna) lighthouse. The brigade started out in that direction and quickly spotted two German cruisers, which were drawing closer to the Russian cruisers. Flagship navigator Sakelari expressed the hypothesis that the enemy was intending to lure the brigade into a minefield. Admiral Kolomejtsev agreed with his navigator and ordered the brigade to turn back to the east.

By comparing the entries, I managed to ascertain that the cruisers Augsburg and Magdeburg and three torpedo boats had the mission of convoying the minelayer Deutschland, with 800 mines, to the mouth of the Gulf of Finland. The cruisers were proceeding ahead, followed at a slight distance by the mine-layer and the torpedo boats. As the Germans were already approaching the designated place for the laying of the minefield, they saw that a brigade of Russian cruisers that was stronger in armament was coming toward them. The German admiral on the Augsburg ordered the Deutschland to depart to the west at full speed. He had decided to join battle with the Russian ships in order to attract them to his own ship, to gain time, and thus to save the minelayer. The German cruisers could always disengage from combat because of their great advantage in speed. And so, when our brigade, unexpectedly for the enemy, avoided contact, the tense situation for the Germans was replaced by one of elation. The Deutschland was immediately returned, and the German admiral reported to his command element concerning the satisfactory completion of the operation.

In view of their avoidance of combat, in which it might have been possible to destroy the German cruisers, or, pursuing them in battle, to overtake the very slow-moving Deutschland, Rear Admiral Kolomejtsev and navigator Sakelari were removed from active duty.

But what *were* the coordinates of the mine obstacle that had been laid by the Germans? The answer to that question was obtained after a study of the piece of paper that I had taken from the radio room. The initial designations that were customary for all radiograms were followed by text consisting of combinations of letters. That prompted me to turn to the signal book. The deciphered top secret enemy report stated that a minefield had been laid at such-and-such a time on 17 August, and indicated its exact coordinates in our waters.

The Fleet Staff immediately reported this information to everyone with a need to know. Our minesweepers checked the position of the minefield and subsequently that field was the first link in a large advance mine position that we gradually created across the Gulf of Finland. During the war many enemy ships found a grave there.

Finding the connection between the German radiogram on the laying of the minefield and the signal book had the most important and far-reaching consequences. It made it possible for the Russian and Allied naval command elements to use the intercepted enemy radio transmissions for intelligence purposes. The COMINT service that we organized consisted, first, in receiving and deciphering the enemy's enciphered radiograms, and, second, in providing bearings

on operating German shipboard radio sets, as obtained by our shore-based radio stations.

A subsequent check of intercepted German radiograms confirmed the fact that the enemy was enciphering his conversations by a combination of literal and digital characters in the signal book. Participating in the exploitation of this material, in addition to Flagship Radio Specialist I. I. Rengarten and myself, were two other persons -- an additional officer and an enlisted-rank radiotelegraph operator -- who were assigned specifically for permanent work in COMINT. It was assumed that the Germans might subsequently change their system of encipherment.

That question was carefully thought out at the Fleet Staff, and the Fleet Commander, jointly with the chief of the communications service, decided to organize urgently a special-purpose radio-interception [*priemnaya*] station in the western part of the southern shore of the Gulf of Finland. To achieve better monitoring of the waves, the site chosen was in the woods, far from populated areas. All the buildings were hidden from outside view and the station's personnel were allowed no contact with the outside world. The necessary supplies were delivered to the station at specified times by car from Revel. The radio station was tasked with only the receipt of German radiograms on several radio receivers. An underground cable connected the radio station with the southern region administration of the signal service. The station's personnel were carefully selected from the officers and the best radiotelegraph operators who knew German. The work of the stations was kept in strict secrecy to prevent the enemy from learning of its existence. Even in the Russian Navy only a few people knew about it.

The Germans used radio communications widely, and soon our special-purpose radio station had accumulated extensive material on various aspects of life, service, and combat actions of the German Fleet.

COMINT helped to keep the command element of the Baltic Fleet well informed on the enemy and made it possible for the fleet, within a short period of time, to change over from the passive waiting for the German Fleet to appear in the Gulf of Finland, to active operations in the southern part of the Baltic Sea.

After a short period of time the enemy, assuming the possibility that his radiograms were being intercepted, decided to make the cipher more complex. For that purpose he began to make it a practice to take the text that had been enciphered according to the signal book and then re-encipher it with the aid of re-encipherment tables [*pereshifrovochnye tablitsy*]. The tables were reissued from time to time. However, that circumstance did not present much of a problem in deciphering the German radiograms. By that time the workers at the radio station had collected extensive material on the basis of the deciphered radiograms. They needed only a few hours to draw up the new re-encipherment chart.

Soon our divers found a second signal book at the bottom of the sea in the area where the Magdeburg had been. At Fleet General Headquarters the book was photocopied and copies were supplied to our Allies, the British and the French.

The Naval Commission for Investigation and Utilization of the Experience Gained by the 1914-1918 War at Sea noted that our COMINT service had achieved great success for several months of the war.

It was interesting for me and the other naval specialists who participated in breaking the system by which the enemy enciphered his radiograms to follow the subsequent development of that case.

The biggest achievement was the ability to use the available materials to create the most commonly used parts of the new signal book after the Germans withdrew from use the old signal book which we had. After receiving the signal book from us, the British also organized a COMINT effort, carrying out similar work in studying German radiograms.

The enemy made wide use of his radio communications. His stations operated constantly. Naval Staff Officer Captain 2nd Rank I. I. Rengarten suggested installing at our coastal radio stations the very simple radio direction finders that he had invented as early as 1912. Following successful testing, the devices were installed at many coastal observation posts where there were radio stations. It was possible to determine the enemy's whereabouts by receiving radio bearings at two points simultaneously.

The time came when the chief of the signal service began to bring to the Fleet Staff a map of the Baltic Sea on which various colors of ink were used to designate the routes taken by enemy ships. Therefore it is not by accident that the Russian ships avoided the German minefields and remained undetected when setting up our own minefields near the German shores.

The command element of the Baltic Fleet made wide use of the COMINT information. The following are a few examples.

The German Naval Staff established a course for their ships to follow when entering or leaving the Gulf of Danzig. On 14 February 1915 two of our torpedo boats laid mines on that course. The very next day COMINT reported that a German transport had been blown up.

We also learned the arrival time of a German cruiser at the port of Libau (now Liepaya) and its departure time. A submarine was sent

to the entrance to the port. As the German cruiser was leaving Libau, it was sunk by that submarine.

Following the occupation of Courland (West Latvia) by the German troops, the German Ground Forces Command which was rushing to seize Riga requested the Naval Staff to provide support from the sea. COMINT revealed these conversations and established the date of the planned operation. The [Russian] Fleet Commander decided to strengthen the naval forces in the Gulf of Riga by sending the battleship Slava. On 31 July 1915 the Slava took the enemy completely by surprise by crossing over from the Gulf of Finland to the Gulf of Riga. COMINT provided such good information about the enemy's plans that when the German fleet, on the morning of 8 August, approached Irbenskij Strait, our torpedo boats and two gunboats were already waiting for them. By 1000 hours the Slava also approached the strait. The Germans' plan to break through into the Gulf of Riga was thwarted.

Early in November 1916, COMINT reported that the enemy was preparing an operation in the southern part of the Gulf of Finland. Information received permitted the hypothesis that

a raid by torpedo boats on Baltijskij Port was expected. The Fleet Staff felt that the Germans should know of the existence of an open passage in the southern part of the forward mine position. The Fleet commander ordered the laying of mines immediately in that passage. During the night of 10-11 November, our radio stations intercepted fragments of conversations between enemy torpedo boats that had suffered a calamity. Two of them had been blown up in the minefields that we had just laid. Then everything became quiet. After approximately an hour and a half, the German torpedo boats began firing on Baltijskij Port. At approximately an hour after that, eight German torpedo boats that were returning to the west came upon the minefield. The flotilla moved along the minefield and then turned to the west again. The torpedo boats began to blow up. During the course of an hour, five of the eight torpedo boats were sunk. All told, seven out of 11 of the newest torpedo boats were sunk.

Thus, by making skillful use of COMINT information, Russian sailors of the Baltic Fleet were, throughout the war, completely aware of the intentions of the enemy's naval forces.

(UNCLASSIFIED)

GEOGRAPHIC NOTE

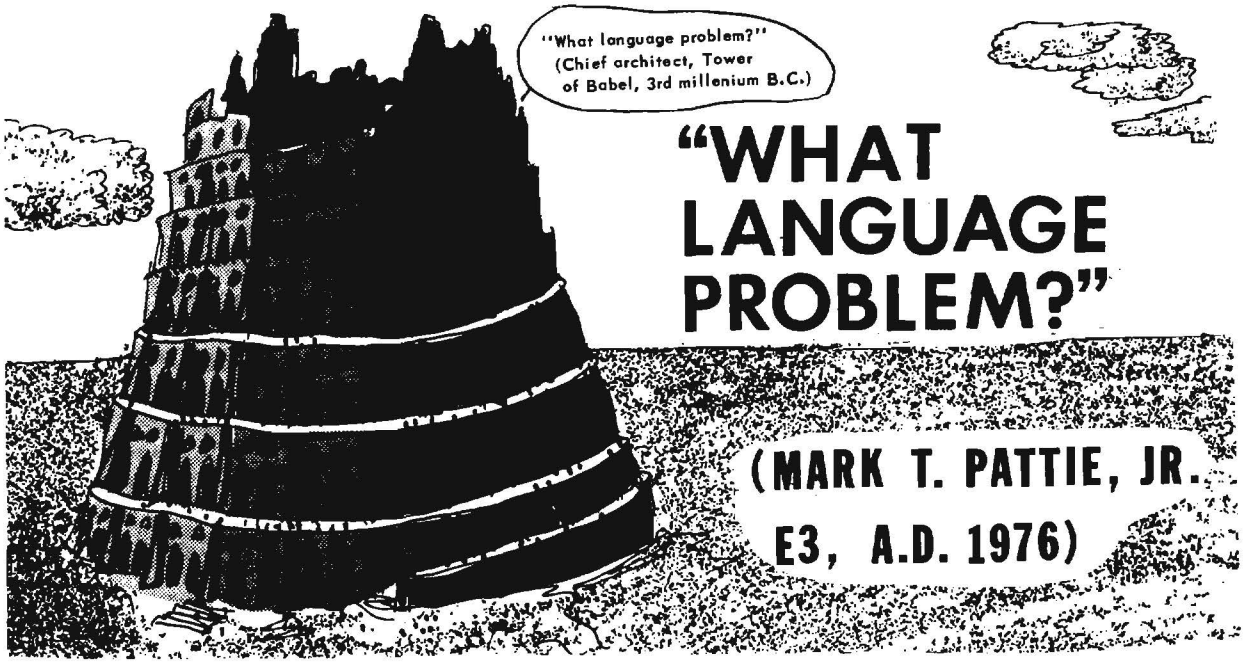
All the geographic names in the preceding article were researched by a geographic analyst in the NSA Geography and Map Library, Room 2N075. That organization also provided the map showing the area discussed in the article, and the following note.

Ed.

The wreck of the Magdeburg, the location of the minefields, and the movements of the Russian and German fleets in WWI naval battles in the Baltic Sea are shown in the *Morskoj Atlas* which is part of the collection of the NSA Geography and Map Library. The reference collection also contains port plans, Russian hydrographic charts with pictures of lighthouses, Soviet Sailing Directions with Notices to Mariners, Lists of Lights and Fog Signals, and the Admiralty List of Radio Signals -- all of which contain a tremendous amount of detailed information.

Baltic placenames are a welter of different languages and variant spellings reflecting the checkered history of the region. Since the U.S. government does not recognize the Soviet incorportation of Estonia, Latvia, and Lithuania, the NIS Gazetteer adheres to the native spellings for *Tallinn* and *Liepaja*. NSA standardized treatment is to transliterate the Cyrillic spellings as *Tallin* and *Liepaya* (irrespective of the native spellings in Latin letters). Until 1917 the Russian names of the Estonian and Latvian ports were *Revel'* and *Libava*. *Odensholm* was the Swedish name of the Estonian island of *Osmussaar* (*Osmussar* as transliterated from the Cyrillic spelling). In 1914 *Tahkona* lighthouse on *Dago* (Russian and Swedish name of island called *Dagden* in German) was renamed *Takhkuna* and the island itself was renamed *Hiiumaa* (Estonian spelling; *Khiuma* in NSA spelling, as transliterated from Cyrillic). *Courland* is one of the former names of the province which became *Kurzeme* when Latvia received independence

(Continued on p. 19)



"WHAT LANGUAGE PROBLEM?"

(MARK T. PATTIE, JR. E3, A.D. 1976)

On 18 September 1975 Lieutenant General Lew Allen, Jr., Director, NSA/Chief, CSS, spoke to the members of the Crypto-Linguistic Association (CLA) in the Friedman Auditorium and used that opportunity to emphasize the importance he attaches to the work of Agency translators. In his remarks he mentioned the high esteem in which Agency translators are held, not only by him but also by those who rely on our product.

The Director's interest in Agency language work is not new, of course, for we have the evidence of the value he placed on the previous year's Jenkins Report on the "language problem" at NSA. Yet this high-level interest seems to have been -- pardon the expression -- lost in translation as it filters down through the levels of management.

Before the Jenkins Report there had been a number of studies of the "language problem" at NSA, but I don't recall seeing any papers showing that a solution was found. Not much earlier than that report, I participated in another, in which I did some research and provided material to the late Dr. Sydney Jaffe for his study. In the fall of 1961 I did research on my own and wrote a report on the problems of retaining college recruits in what was then B1, with the report going to M3 through Dr. Jaffe. The bulk of that report was concerned with the hiring and retention of linguists. Originally I myself was hired as a linguist, became a book-breaker, and then went on to other forms of cryptanalysis and into management, so I do have some personal experience on the "language problem."

When I was hired it was because I could translate from what is still considered a "rare" language, and this was when people were being released from their jobs because of cutbacks. Now, many years later, the Agency continues to seek people with linguistic ability even when hiring has almost stopped. This is certainly a strong indication that the Agency does have a real need for people who can translate well. It also means, to me, that the Agency is not able to retain enough qualified linguists to do the necessary jobs, for recruiters are constantly reminded to keep their eyes open for someone who is already able to translate a particular language or who can be easily trained to do so. But why, then, do translators leave the work?

Perhaps the problem is not in our hiring practices or in our training, but in the failure to recognize what the value of a good translator is. In recent years I have been quite surprised to see so many of our most skilled translators leaving well before they had reached the mandatory retirement age. The few I spoke to told me that there was just nothing they could do to overcome the feeling that what they were doing was regarded by those above them as of little value to the Agency. The "important" work is being done by engineering and scientific personnel. That there may be some truth in their statements can be seen in an examination of promotions to GGD-13, 14, and 15 during the 1974 and 1975 calendar years. The Agency's own statistics, as can be seen from the following table, point up the fact that anyone wanting to be promoted to the higher grade must get into a field such as Electronic Engineer, Data Systems Analyst, Cryptologist, or Cryptologic Staff Officer.

Promotions to					
GGD-13		GGD-14		GGD-15	
CY74	CY75	CY74	CY75	CY74	CY75
Total promotions:					
Including:					
Special Research Analysts					
Electronic Engineers					
Data Systems Analysts					
Cryptologists					
Cryptologic Staff Officers					
Linguists					

P.L. 86-36

Parenthetically, Special Research Analysts can scarcely find comfort from the relatively high figures for promotions to GGD-13, because that grade seems to be the end of the line for most SRAs (including linguists posing as SRAs for promotion purposes).

But what about the linguists who do not want to pose as anything that they aren't, but just want to continue working as, and getting promoted as, *linguists*? Most of them find their niche one grade lower, and reach the end of *their* line at GGD-12. Only a token few move higher. Why? The career structure allows for linguistic jobs at higher levels, but, to my knowledge, only one person with the label of linguist has a grade higher than GGD-15, and he was promoted over 10 years ago.

No, it is not that the structure doesn't permit promotions within the linguistic field, so the answer must lie elsewhere. I see no other place to look for the answer than in the attitude of Agency management towards language work.

In too many cases, managers of linguists have had no language experience of their own and tend to think that any job requiring the knowledge of a foreign language must be fairly simple. And yet the Crypto-Linguistic Association has, over the years, held several symposia and given several presentations in the auditoriums at Fort Meade and FANX, dealing with various problems encountered by the NSA linguist -- problems of language recognition, transcription, translation, machine processing, teaching, testing, etc. Agency linguists have, over the years, written numerous articles for the *NSA Technical Journal*, the *NSA Cryptologic Spectrum*, and *CRYPTOLOG* (or its predecessors *Keyword*, *Dragon Seeds*, *QRL*, *Command*). Have the managers attended the symposia? Have they read the articles? Are they reading *this* article?

Even as I write this, I have been told of a senior manager who feels that translation is "journeyman" work which can be handled by high-school recruits, after some training. Somehow I have the feeling that all the words that have been spoken and written have made no impression, that only linguists read articles about language, and that no one else really cares.

I think it is safe to assume that the attitude expressed by that senior manager is more typical than not. Lack of promotions is certainly evidence of this. In the face of such obvious coolness toward their field, only the most dedicated linguists will persist in the work. The majority will seek jobs in other fields or will leave the Agency for positions in which their linguistic talents will receive the proper respect. In either case the Agency will continue to have a "language problem."

There are some ex-linguists in management jobs in NSA, but few are in positions where they can continue to make use of their language skills and knowledge. One such exception is the National Cryptologic School, but only because it has a department whose mission is language teaching -- even in this instance, however, the Department Head is listed not as a linguist, but as a Cryptologist. Another exception I am aware of is P16, and the head of that element is a Cryptologic Linguist. Again, though, since P16 is exclusively devoted to linguistic matters it could scarcely be headed by anyone other than a linguist. There may be

other positions, such as overseas, but I think that the point stands.

I guess that what I am really trying to say is that there is not enough recognition given to linguists, and for me recognition means promotions and important jobs. More of those who are truly professional should be promoted without having to change jobs. More linguists should have the managerial roles over elements where the mission is largely language-related. Too many of the people who are now in such positions have little or no understanding of what it takes to be a translator -- or a voice interceptor, or a transcriber, or a teacher -- and they don't seem to care. To say that they are unsympathetic to linguists is to put it mildly.

When linguists are appointed to jobs in the upper management levels, they will be in a better position to counteract the negative attitude held by too many of our current managers. Then and only then will I believe that the "language problem" is on its way to being solved.

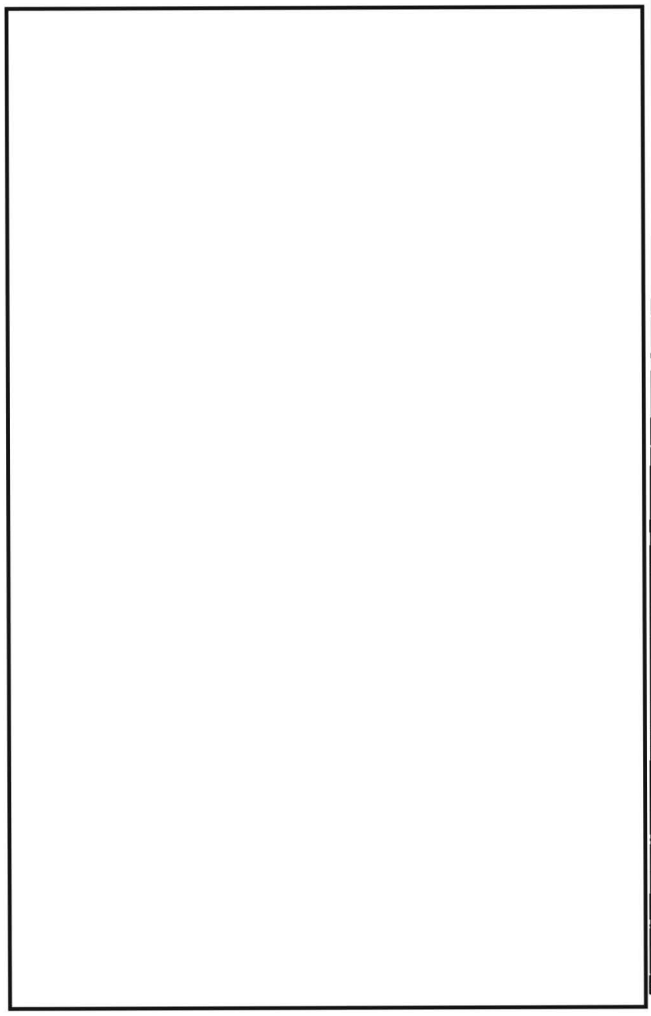
~~(FOUO)~~

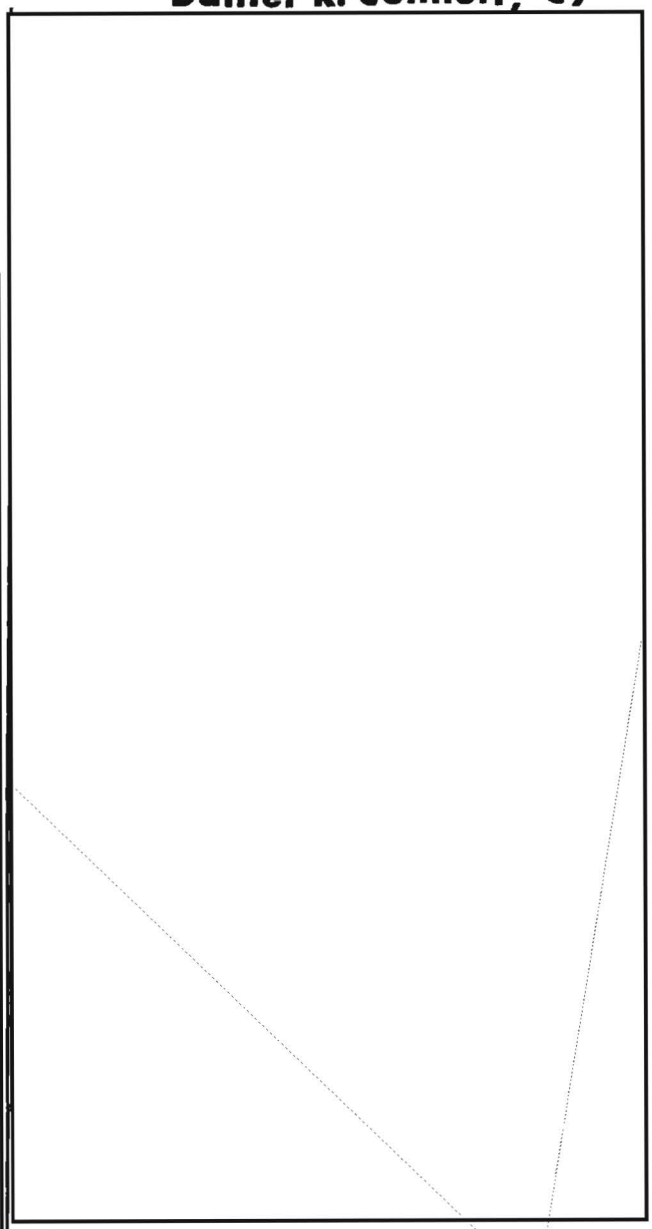
WHAT'S WRONG WITH AG-22/IATS?

Daniel R. Connell, C7

In the March issue of CRYPTOLOG we reprinted the article "Musings About the AG-22/IATS," by Cecil Phillips, C03, which had originally appeared in C-LINERS (C Group Machine Processing Information Bulletin), Vol. 3, No. 7, August/September/October 1975. Mr. Phillips' article prompted the following reply by Daniel R. Connell, which appeared in the Winter 1976 (Vol. 3, No. 8) issue of C-LINERS and is being reprinted here with the permission of its Editor, David J. Williams.

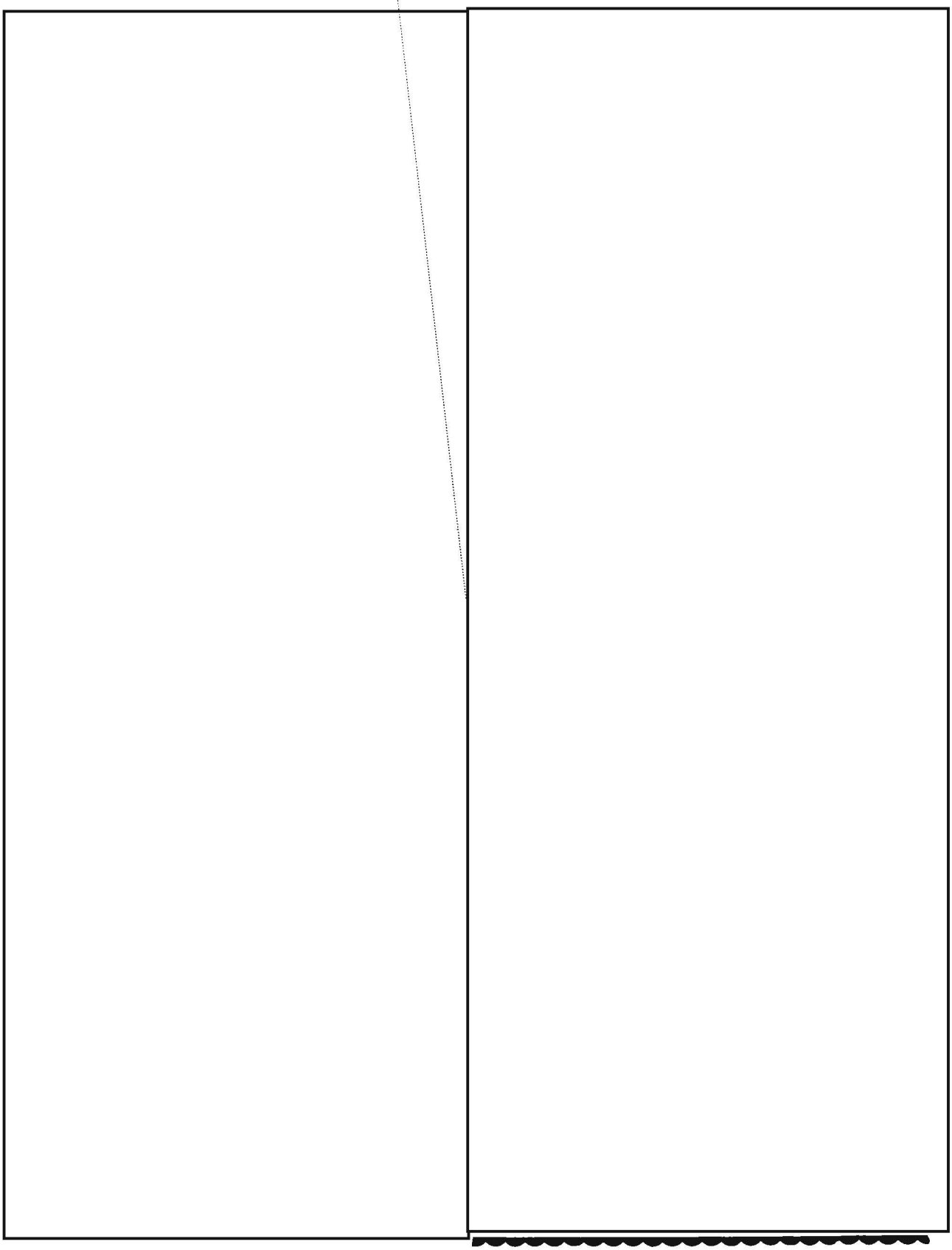
Ed.

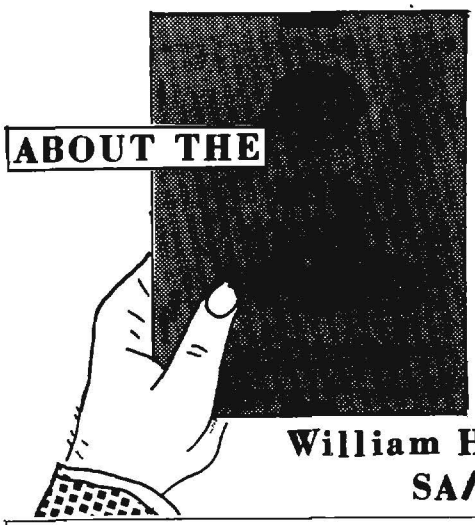




~~(CONFIDENTIAL - HVCCO)~~

~~CONFIDENTIAL~~





William Hunt, SA/DDF

The following article was written by William Hunt when he was developing the SIGSUM. It appeared in the February-March 1973 issue of the Agency publication KEYWORD: Technical Exchange Bulletin *(now discontinued).*

The SIGSUM has served NSA well during many crisis situations, by bringing current SIGINT items to the attention of senior U.S. officials in the United States and overseas in capsule form -- the function for which it was primarily designed.

Ed.

The NSA SIGINT Summary (SIGSUM) is a daily publication conceived and designed by the Assistant Director for Production to inform selected senior executives of the United States Government, both military and civilian, of the most significant world developments as seen in SIGINT. Second-Party cryptologic collaborating countries also receive the publication for their use as appropriate.

While this publication was conceived as early as 1964, it was not until the past two years that it was fully developed and its objective and utility fully appreciated; as of today, it is one of the most widely read documents at the CAT III level in the SIGINT-indoctrinated system.

While it is neither possible nor desirable to trace the growing pains of the Summary suffice it to say that it suffered the usual development of any document for which no clear-cut requirement existed. NSA Production recognized the need for such a vehicle to alert selected senior U.S. executives to important items of interest in capsule form, to explain the COMINT fact, to interpret the communications activity, and to report it in meaningful terms. From the customer's point of view there was an understandable suspicion that this document would overstep the mythical line between reporting the SIGINT and evaluating it. It can be readily seen that misunderstandings, semantics, and the efforts of well-intentioned people in NSA and customer organizations would cause problems until all parties understood the philosophy and responsibilities of each other's roles and missions and learned to appreciate and adhere to the basic principles of their respective missions. All of these problems appear to be resolved, and with the exception of an occasional human error no future major differences are anticipated between NSA and its customers regarding the Summary.

As previously stated, the SIGINT Summary is a daily Production publication covering all SIGINT problems of NSA Production at the Category III level. It is released at approximately 1700 local time each day by electrical means and is disseminated to ZI addressees on the NSA SIGINT electrical system. It is also transmitted to selected overseas major military commanders, NSA/CSS field offices, and specific cryptologic organizations. Second-party cryptologic collaborating centers receive the electrical copy.

The hard copy of the SIGSUM is designed for the executive reader who does not require timely electrical receipt of SIGINT items. It is available on his desk daily at the opening of business and contains the SIGINT available to NSA at approximately 1700 the previous day. During crisis periods and/or when an item is of sufficient importance to warrant distribution by electrical means more frequently than daily, an item is prepared and if ready for publication after 1700 hours is released as an advance item to the next daily SIGSUM.

Items appearing in the SIGSUM are never original items. By this is meant that all analysis is performed by the Production organizations having total responsibility for a specific problem. If and when a SIGINT report or item is developed by an analysis organization of Production it is serialized and distributed in accordance with established requirements and procedures. Simultaneously, an abbreviated item is prepared suitable for inclusion in the SIGSUM and forwarded to the SIGSUM panel for editing, processing, and distribution to recipients as explained above and in accordance with SIGSUM policy procedures. In all instances the serial number of the complete report is cited in the SIGSUM to assist the customer who must have the complete details for evaluation or estimative purposes in acquiring the unabridged report. The complete report on which the SIGSUM item is based normally reaches the recipient before or simultaneously with the SIGSUM item; therefore those recipients who need the complete details will have them available.

Since the SIGSUM is designed for selected senior executive readers, it is published six days per week, Sunday through Friday. This insures that readers working Monday through

Saturday will have the relatively latest SIGINT available each working day.

For the convenience of the readers, appropriate maps are included in the hard copy of the SIGSUM with notations and overlays showing the precise areas of activity as reported in the item. On occasion, photographs of military weapons or weapons systems are included primarily for the benefit of readers not familiar withese weapons. Photographs of weapons and weapons systems include ship types, sumbarines, aircraft, tanks, radars, missile systems, artillery pieces, etc. On occasion, photographs of personalities are also included.

In addition, selected collateral is included when it enhances the SIGINT or assists the reader in understanding it. In all instances where collateral is utilized it is so flagged in the item. In hard copy, collateral is printed in italics.

In instances where foreign collaborating centers have responsibility for reporting on a target and/or where unique SIGINT is available to them, such items as appropriate will be included in the SIGSUM, citing the foreign cryptologic collaborating organization's serial number and/or appropriate caveat to inform the reader that such an item is not produced by a U.S. cryptologic organization.

Senior military commanders overseas have expressed their interest in this document as it provides them with an appreciation of the level of military activity in other areas of the world and assists their intelligence staffs in evaluating military activity in their own areas. Intelligence staffs worldwide have found the SIGSUM valuable because of the brevity of the articles and their suitability for general briefing purposes.

~~(SECRET - HVCCO)~~

SOLUTION TO LAST MONTH'S NSA-CROSTIC:

Lambros Callimahos, "[The] Rosetta Stone [and Its Decipherment]," *NSA Technical Journal*, Vol. XVI, No. 1, Winter 1971.

"I feel particularly qualified to give this lecture because . . I was born in Egypt . . . Furthermore, the Ptolemies were Greeks. . . . Ptolemy V was five years old when he ascended to the throne, and I was four years old when I first set foot on the American shore, so you can see the similarities."

(UNCLASSIFIED)

SOME PRINCIPLES OF COVER AND DECEPTION

P.L. 86-36

Vera Filby's article ("How Do We Know It's True?") in the February CRYPTOLOG is a most interesting one and should stir substantial comment and thought.

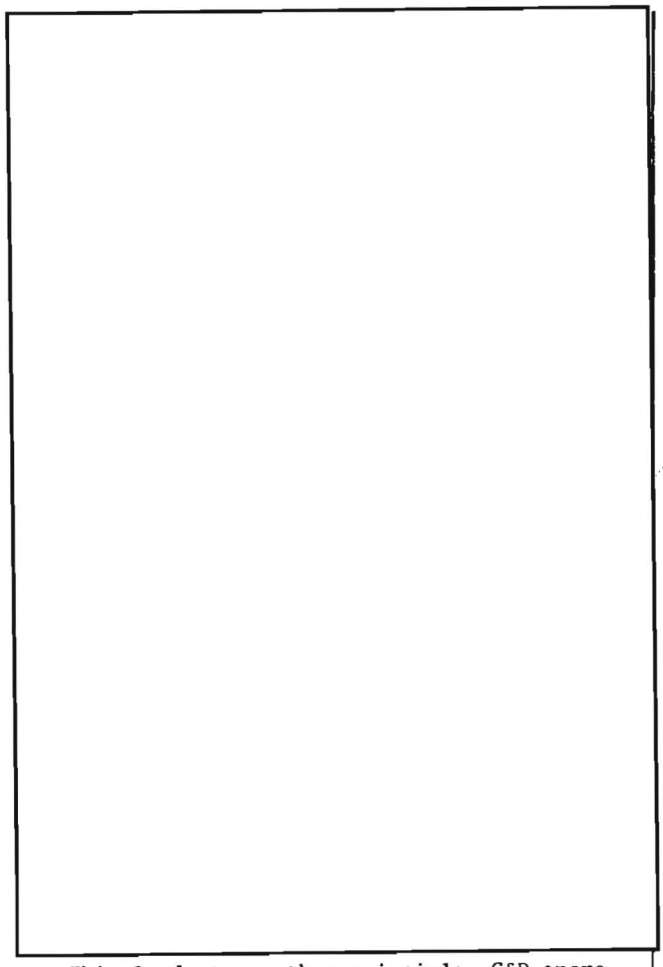
The article's publication is timely, inasmuch as it appears coincident with a new two-volume work by an English journalist, Anthony C. Brown, entitled *Bodyguard of Lies* (Harper & Row, 1975). Mr. Brown has done a good job of recounting the uses and successes of Allied cover and deception (C&D) operations in World War II. His story is set in a broad framework that includes key personalities, leading interests, and many of the apparent motivations and relationships which culminated in C&D operations. Understandably, the book emphasizes the role of Great Britain, starting with its title, which reflects a statement attributed to Prime Minister Winston Churchill: in wartime, he said, truth is so vital that it must be attended by a "bodyguard of lies." The small coordinating body which ran the British C&D effort reported directly to Churchill for reasons of both security and span of control.

C&D, in general, seems to have some principles that are worthy of iteration: first, and certainly foremost, is the principle of absolute and unassailable secrecy. Because commanders, with their operations and intelligence people, are often sensitive to being deceived, it is frequently true that the slightest hint that deception is being practiced or even planned is sufficient to abrogate the C&D operation as well as to heighten suspicion in the future. Accordingly, *all* actions taken to do things to and about C&D must be done with utmost circumspection. In that vein, the symposium which Ms. Filby recommends should be pursued with all due regard to "must-know/need-to-know" criteria. What Ms. Filby recommends, as I read it, is a symposium attended mainly by SIGINT people and some SIGINT users, to look into the question that the title of her article asks.

This leads to two more C&D principles:

- if a C&D operation works ideally -- or even reasonably well -- we either do not know that we are being deceived or cannot prove (or even hypothesize) it; and
- C&D operations, for the most part, are not limited to electrical communications alone, but also involve one or more levels of forces and units.

~~(SECRET - HVCCO)~~



This leads to another principle: C&D operations, of various magnitudes and kinds, happen not only in wartime, but also in *peacetime*. It is not an unreasonable assumption that they are being carried out right now.

A fifth principle of C&D is one which I might nickname the "ours/theirs" principle. In essence, it describes an existing condition in which both, or all, adversaries practice some C&D, and both, or all, simultaneously attempt to fathom all other C&D. I mention this aspect because it is that one condition that most easily leads to self-deception. By that I merely mean that it is important to keep straight who is doing what to whom when and for what reasons. If one element of the organization is supporting friendly C&D and another element is attempting to peer through an enemy's *possible* C&D, and there is no central coordinator, the self-deception that can result will compound the real deceptions. Interorganizational and intraorganizational work groups and symposiums can overcome some of the difficulties inherent in this potential problem, but they cannot take the place of a central, authoritative, coordinating body.

The last principle that seems worthy of mention is that of *surprise*. It is one of the hallowed "nine principles of war" and harkens back in history immemorially. It is inexorably bound up in the business of C&D and is frequently that which C&D operations seek to advance. It might be of interest to recall that contemporary Soviet publications dealing with military strategy and tactics are rather liberally laced with detailed discussions of the element of surprise. In several instances, those discussions are detailed enough to make it clear that the Soviet have assigned significant importance to that particular aspect of military operations. As might be expected, that literature contains associated references to C&D less frequently, but those references are not altogether absent, either explicitly or inferentially.

In my view, which is shared by some of my contemporaries, Ms. Filby's basic question, "How do we know it's true?", is of central, compelling criticality in today's U.S./Allied intelligence community, especially in the signals intelligence part of that community, where there is sometimes a tendency to place increasing credence in and dependence upon limited, decreasing signals sources. Our understandable tendency to rely on what we have -- however tenuous it may be -- can be used against us, and with dire consequences, in time of war. Our national defense strategy is increasingly dependent upon "indications and warning" (I&W) intelligence. There is nothing wrong, in any way, with that dependence, *provided we understand and can resolve the problem addressed in the Filby article*. I believe the problem is recognized and understood in some quarters, but not as widely as it might be. I believe that to deal realistically with the problem, considerably more attention is warranted. I would start by establishing a single, central, coordinating group with defined authority to work across organizational boundaries. The initial objective of that group would be to assess the magnitude, dimensions, and impact of the problem. If the problem is found to be of sufficient size and consequence, the next step would be to organize the attack on it. A modest number of additional man-hours may then be warranted. Some priorities may have to be changed to identify and task those man-hours. The first "product" out of that effort probably should be directed toward our own current reporting, to strengthen the value of I&W intelligence.

To the extent that this "science" now has an epistemology, it is inexact. Our current understanding is, at best, inconclusive, in part because it is not yet organized. In point of fact, how do we know "it" is true?

~~(SECRET - HVCCO)~~

CONVERSATION WITH A BOOKBREAKER (SINCE RETIRED)

[redacted]

~~(SECRET - HVCCO)~~

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

TRANSLATORS' COMPENDIUM

The sample pages on the opposite page are reproduced from the NSA/CSS publication *Collected Articles on Translation, 1973*, compiled by [redacted] (TSC). Mrs. [redacted] three-sentence foreword "says it all": P.L. 86-36

> *The following articles, which first appeared in QRL, Keyword, Spectrum, the NSA Technical Journal, [Dragon Seeds, and CIA Studies in Intelligence], have been selected for their bearing on the subject of COMINT translation as seen through the eyes of practioners of the art. Together they represent the experience of a generation of Agency linguists. They are here reproduced in the hope that they will interest and stimulate another generation.*

The publication contains more than 500 pages and is divided into seven sections, plus a bibliography. The section "Training for Translation" has articles by Doris Miller, Emery Tetrault, [redacted] and [redacted] "The Translator Helps Himself" has articles by [redacted] Mary Roberta Irwin, Stewart H. Buck, Robert E. [redacted] Norman Wild, and John D. Murphy. "Preparing the Text for Translation": [redacted] "Problems in Translation, General and Specific": [redacted] A. J. Salemme, [redacted] P.L. 86-36 James Duncan, and Jack Gurin. "The Erring Translation, and What to Do About It": Harry G. [redacted] Dr. Marion Griggs, [redacted] Doris Miller, A. J. Salemme, [redacted] Barbara Dudley, Stu- [redacted] Donald Lasley, Norman Wild. "Machine Translation": [redacted] [redacted] A. J. Salemme, Doris Miller, Norman Wild. "About Translators and Translations: A Miscellany": [redacted] Barbara Dudley, [redacted]

The subjects covered in these articles are still current ones. For example, every week someone becomes newly agitated about the problems of transliteration or of machine translation, but is unaware that the ground has often been covered before. For that reason, this reminder is being printed, so that the new generation of linguists can be aware of the existence of this record of other linguists' efforts.

A few copies of the publication are still available. If you would like a copy, call [redacted] P16, x4998, Room 3W076. Reference P.L. 86-36 copies are available in the Cryptologic Library, Room 3W076, and in the NSA Technical Library.

THE CREATIVE TRANSLATOR

by [redacted]

"It is essential that the captain take steps to assure an attack as soon as possible," the translation read. "No delay will be accepted." I knew that the text in question has been passed in the heat of battle, by a man desperate in the face of imminent defeat and possibly death. It struck me that his language was rather formal for the occasion. [redacted] I would have translated it, "Strike soonest without fail. ((Time)) is of the essence. Any delay will mean failure." The first tr[illegible]lation was not wrong, It simply missed the point.

The example is an extreme c[illegible] altered to protect the guilty), tendency of translators to smoc[illegible] original, to impose order and [illegible] everything in unruffled govern[illegible] destroy the vitality of the o[illegible] it. In so doing, we do our c[illegible] say nothing of insulting thei[illegible]

This article, then, is [illegible] lation. Unlike other disci[illegible] answer, translation plunges [illegible] ambiguity where there are [illegible] right ones. The choice of [illegible] depends not on dictionarie[illegible] gence, emotion and unders[illegible] language, which is first [illegible] ably tied to feelings in[illegible] and heavy with emotional[illegible] means of information co[illegible] darkness. And as any l[illegible]

confusion among linguis[illegible] tor [redacted]

the people taking a[illegible] few years ago. It [illegible] material and one of [illegible] been [redacted]

graphese). Several [illegible] ad real trouble trying t[illegible] Out of admiration. . ." o[illegible] so wrong.

But the problems caus[illegible] pared to the problems g[illegible] marks. Sometimes it [illegible] he end of one sentence [illegible] There is the classic

DORIS MILLER

~~TOP SECRET UMBRA~~

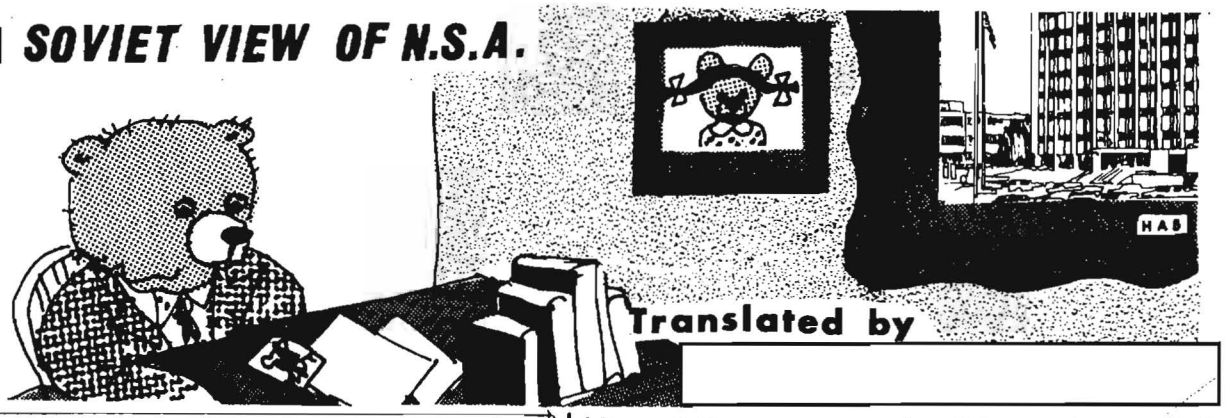
~~TOP SECRET UMBRA~~

LEARNING FROM MISTAKES

By Mary Roberta Irwin, G543

[redacted]

A SOVIET VIEW OF N.S.A.



Translated by

Translator's note: *A recent Soviet book on SIGINT (*Radioehlektronnaya Razvedka *(Radio-electronic Intelligence), V. A. Bartanesyan, Moscow, Voenizdat, 1975) is evidence of a Soviet effort to heighten awareness of the vulnerabilities of electronic emitters among all those who work with them. Two hundred fifty pages long and citing 70 titles -- mostly U.S., British, and German books and periodicals -- as sources, the book outlines the organization and scope of the U.S. SIGINT effort and its technical capabilities. It is, in effect, a SIGINT primer.*

Chapter I is introductory and general, sketching out the structure of U.S. SIGINT and its place in intelligence, recounting some anecdotal WWII SIGINT history and summarizing its postwar development up to the present, including the growth of SIGINT collection by satellites. Chapter II discusses the exploitation of the various portions of the electromagnetic spectrum, and Chapter III treats antennas. Chapter IV is devoted to signal search, intercept, and analysis equipment. The fifth and final chapter is on direction finding.

The tabloid-style description of NSA given in Chapter I might almost seem to have been written tongue-in-cheek if the broad irony of certain assertions could be accepted as being truly intentional and not simply accidental. The following is a translation of that description.

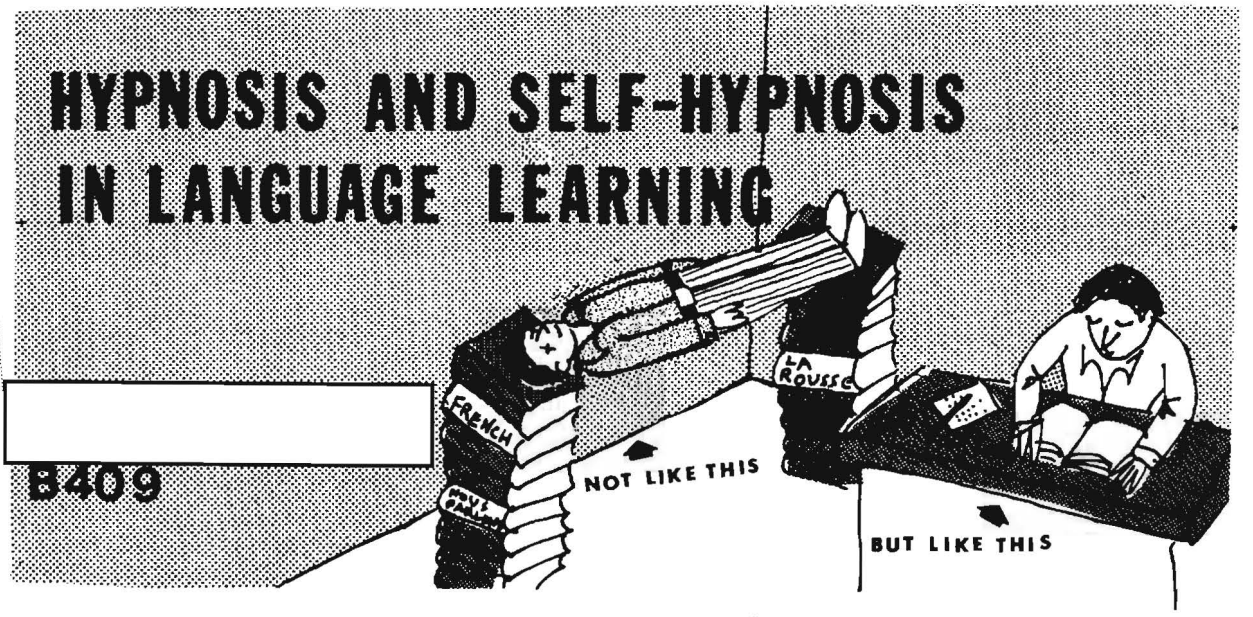
The NATIONAL SECURITY AGENCY (NSA) is one of the largest intelligence organs in the United States. NSA occupies a special place in the general system of global espionage. It informs the President and other high-ranking persons concerning the political and economic situation and the defense posture of many countries of the world, including the allies of the United States. The entire work of NSA is highly classified. Only rarely does information of the doings of NSA appear in the bourgeois press. Nevertheless, from the fragmentary information that gets published some idea of the enormous scale of its spying activity can be formed. NSA Headquarters is located at Fort Meade, midway between Washington and Baltimore, in a huge three-story building that is second only to the Pentagon and State Department in size. P.L. 86-36

NSA is the chief SIGINT agency and has unlimited financial and technical capabilities. NSA's long tentacles of radioelectronic espionage reach everywhere. Created in 1952 by a presidential order of President Truman with the obscure explanation that it is "charged with carrying out highly specialized functions involving the national security of the United States," NSA has developed into an enormous SIGINT service. Its annual budget is over a billion dollars, and its staff of employees at the Headquarters alone is 14,000. Three or four thousand employees work abroad, and about 20,000 service personnel who are formally subordinate to other intelligence organizations are in fact engaged in SIGINT work in behalf and under the control of NSA.

NSA conducts radioelectronic espionage from ground centers (military bases), piloted and pilotless aircraft, naval surface vessels and submarines, and from satellites equipped with appropriate radioelectronic gear. NSA uses universities and the research laboratories of various industrial corporations to find solutions to various technical problems and to build improved SIGINT collection apparatus.

The functioning of several major departments is known from the foreign press -- Operations, Scientific Research, Communications Security, and others. The largest is Operations, which is engaged in processing the data collected and received from all SIGINT collection points, deciphering it on the basis of engineering cryptanalysis, and compiling operational reports. The focus of attention of Operations is on deciphering the governmental and diplomatic codes and ciphers of various countries, as well as the codes and ciphers used by the armed forces of those countries.

NSA Headquarters has a large electronic computer center supporting the computer operations of all the major departments of NSA.



In this article I won't be conjuring up images of Svengali or Dracula, or discussing hypnosis as stage entertainment or as depicted in highly fictionalized TV plays. Nor will I be discussing the deep stages of hypnosis as used for medical purposes, such as in childbirth, to replace a chemical anesthetic. Instead I shall be discussing hypnosis and self-hypnosis as a language-learning tool, for which a relatively light state of relaxation is sufficient.

Because relaxation is really what hypnosis is all about. Sorry about that, but hypnosis does not really involve mystic trances. It won't bring you back to a previous incarnation, force you to become unwillingly involved in crime, and, above all, it won't cure anything -- except, possibly, insomnia. Hypnosis is no more and no less than a heightened state of relaxation, self-induced or induced with the aid of a hypnotist, during which you are considerably more open to suggestion than when you are "awake." Why the quotes around "awake," did you ask? Because it is a word that hypnotists use to differentiate between being hypnotized ("asleep") and *not* being hypnotized ("awake"). Actually, however, hypnosis is not sleep in the natural sense -- there is no loss of consciousness, no trip to Never-Never Land, no loss of contact with the hypnotist or the surroundings, no sense of being in a trance. The only thing you feel when hypnotized is relaxation.

Most people have become hypnotized in the sense that they have succumbed to a suggestion that slipped into their subconscious mind while their conscious guard was down. If I start telling you about sucking on a lemon, I'll bet it won't be long before your mouth starts reacting! Or if I start yawning in a crowded room, it won't be long before someone else starts yawning. Sometimes, though, it doesn't take another person to get you going. When was the last time that you decided to buy an item displayed at the supermarket checkout counter, even though you didn't need it? The point is that we are all subject to suggestion and autosuggestion. Hypnosis (which, incidentally, was named after the Greek god of sleep, Hypnos) simply formalizes that idea and is a way to make the character trait of suggestibility a positive rather than a negative feature.

But enough introduction! Let's get into that language classroom!

Even though the student wants to be there (or says that he wants to be there), the language classroom is basically a hostile environment for him. The student's motivation for learning may be affected by years of adverse conditioning, of which he is not even aware. He is going to be faced with new behavioral problems. He might be so introverted that he will feel embarrassed and even say, "I can't do it!", when asked to articulate the "funny sounds" of the foreign language. He may lack confidence in his ability to memorize large numbers of foreign words or grammatical rules, or, when learning certain languages, to figure out how the language works with little or no formal structure. Finally, and probably most important, he is under stress and pressure that he could not have easily calculated. Unfortunately, almost none of these problems will be taken into account within the language class proper. Nowhere in the curricula is there a mention of classes in relaxation, concentration, motivation, or mental conditioning. And yet there ought to be such classes, because it is just as easy to condition the mind as it is to condition the body.

So let's do something about it! Just about every reasonably intelligent person can learn a foreign language (as just about every reasonably intelligent person can be hypnotized). Many people who say they cannot learn a foreign language (as many people who say they cannot be hypnotized) are really saying not that they *can't* do it, but that they *won't* do it. No language teacher can *make* you learn those grammatical endings, just as no hypnotist can *make* you relax. You have to want something, and you have to cooperate. All right, then, do you really want to learn the language? If so, here are a hypnotist's suggestions to help you learn it quicker and better.

I would like to focus on the following five areas:

- relaxation,
- concentration,
- confidence,
- motivation,
- mental conditioning.

I shall limit myself to the hypnotic methodology, although much of what I will cover is common to all types of relaxation therapy.

Relaxation

This does not happen automatically, but it can be learned, sometimes just by picking up a book on the subject and following instructions. Most often, however, the student needs some kind of instruction in relaxation. With hypnosis, he will usually attend about eight sessions. After the initial visit, which I shall describe elsewhere in this article, he will attend as a member of a small group. Those remaining sessions will be more or less identical, except that special problems may receive added emphasis. The hypnotist will hypnotize the group all at the same time and begin making his suggestions. He will start with suggestions of relaxation and will deal with such as ideas as relaxing without slowing down; coping with stressful situations; maintaining composure under difficult conditions; relaxing while alone or with others, friends or strangers; and conditioning intended to convinc the subject that he can relax under any conditions at will. He will mention the benefits of such a capability, emphasizing that tension steals energy. The hypnotist will stress the need for restful sleep and suggest that the student will indeed sleep restfully and wake up every morning feeling refreshed and eager to get going on the new day.

The ways in which these suggestions can help the language student are far-reaching. He can relax in the classroom when it is his turn to speak those "strange-sounding" words; he can overcome the general nervousness and embarrassment he feels when he makes mistakes, and be composed enough to correct them; he can relax when doing his language homework -- memorizing words or learning grammatical rules; and he can pay far better attention to what is going on in the classroom. Instead of nervously worrying about his own performance, he will be learning from the performance of everyone in the class, not just himself.

Concentration

As I just mentioned, the calm individual pays better attention to what is going on around him. Because he can relax, he can concentrate his attention better on the job at hand. The suggestions that the hypnotist can make in this area center on: better concentration through relaxation; getting a stronger impression from the material studied, so that retention and recall are easier; improved memory; better organization of time and efforts, with less procrastination; accomplishment of the things the student wants to do and has to do.

The language student can apply these suggestions primarily in his classroom participation and homework study. He will be able to tune out distractions at both times, making his efforts more productive and pleasurable.

Confidence

Here the hypnotist will work against any adverse conditioning that may be present. He will make suggestions designed to strengthen the student's confidence in his ability to practice self-hypnosis; in his ability to cope with any set of circumstances; and in his ability to absorb the complex material being studied.

And how will the language student apply these suggestions? He can apply them in every area of language study, but perhaps more than any other suggestions, these will work on a subconscious level to make the course more productive for him. A student is not always aware of adverse conditioning that may have taken place previously. He may think that he is "not particularly good at languages," because of impressions made upon him as early as elementary school. He may feel that his intellectual capacity is much lower than it actually is, or consider the language material more complex than it actually is. Through hypnosis and self-hypnosis he can change that kind of negative thinking, he can "recondition" himself and learn to appreciate his true capabilities. While humility is a fine characteristic, we already have enough humble linguists, and sometimes the difference between the good linguist and the great one is no more than the confidence to cross the line between translating something as "swelling of the thyroid gland on the neck" or as "goiter." In other words, the confidence to let go of the literal translation and to make the translation read as well in English as it did in the original foreign language (maybe even better!).

Although it will almost certainly follow that the relaxed, concentrating, confident student

will be a better student, the hypnotist will reinforce suggestions of motivation. He will reinforce the ideas that relaxation saves energy, reduces or eliminates tension, and makes sleeping easier and more restful; that better concentration strengthens the initial impression that the student receives from the study material, improves retention and recall, and motivates the student toward better-organized efforts; and that the student will be confident of success.

Although it is probably the most elusive of animals, motivation can be caught and tamed. "Nothing succeeds like success" may be a cliche but that doesn't make it a false statement. The more language a student learns, the more he is likely to learn as he goes along. What he often needs is an extra charge of steam at the beginning of his language course, when he has serious doubts -- often bordering on panic -- that he will ever be able to master this impossible language. Those doubts can be eliminated, and if we do that, we go a long way toward reducing the high attrition rates that are usually associated with language training.

Mental Conditioning

Unless the student learns to practice some form of mental conditioning on his own, the whole purpose of hypnosis is defeated. Posthypnotic suggestion by the hypnotist does not last forever. Therefore the suggestions made by the hypnotist must eventually become suggestions reinforced through self-hypnosis by the student himself. He will be told while hypnotized that he can bring about this same state of relaxation by himself, usually once a day just before going to sleep at night. During the day he will reinforce the suggestions by repeating keyword suggestions ("Relax," "Concentrate," etc.) to himself. These are designed to produce a conditioned response of calmness, concentration, confidence, etc. An important distinction here is that the student will not be hypnotized or enter any "trance" during the day. Rather, he will have conditioned himself to respond to the suggestions while awake, that is, posthypnotically.

How to Do It

It all sounds so easy, so why isn't everyone doing it? Actually, a great many people throughout the world are already involved in this or similar training, but usually on an individual basis, that is, one person attempting to improve his performance in a given area. Literally hundreds of thousands of Americans are currently involved in self-hypnosis, meditation, biofeedback, transactional analysis, or some form of relaxation therapy, trying to do everything from easing the strain of a high-pressure job to shaping up an entire baseball team. So why shouldn't a language student try it too?

Let's say that he *does* try it, with hypnotism. He walks into the hypnotist's office. What happens then?

The hypnotist has an initial private session with the student. During that session he tests the student for suggestibility, imagination, and subject type, all of which information tells the hypnotist what are the best methods he should use. He also shows the student how hypnotism works, but does not actually hypnotize him at this time. Instead, he uses various "waking tests," such as asking the subject to hold both arms straight out in front of him and then suggesting, with appropriate words and appropriate vocal modulation, that the right arm is very heavy and the left arm is very light. Or he will stand behind the subject and tell him to think about falling back, knowing that the hypnotist will break his fall if necessary. Either with or without further suggestion by the hypnotist, a suggestible subject will usually start swaying on his heels within a few seconds.

The hypnotist and the student then discuss any questions, general or specific, that the student might have about hypnotism, and the particular problems he is having in language learning.

After the tests and the discussions, the hypnotist uses an appropriate method to hypnotize the student, using no more than a couple of minutes to do so. In addition to implanting suggestions designed to improve the student's learning, the hypnotist makes suggestions designed to produce greater depth of hypnosis during subsequent sessions and to condition the student for the group-induction method that will be used in future sessions. The hypnotist also tests the student by implanting a posthypnotic suggestion. This is done for two reasons: to prove to the student that he was actually hypnotized (the feeling of relaxation alone is sometimes not enough to convince persons that they have been hypnotized); and to give the hypnotist some idea of how quickly the student will respond to further hypnotic suggestions. And that ends the first session.

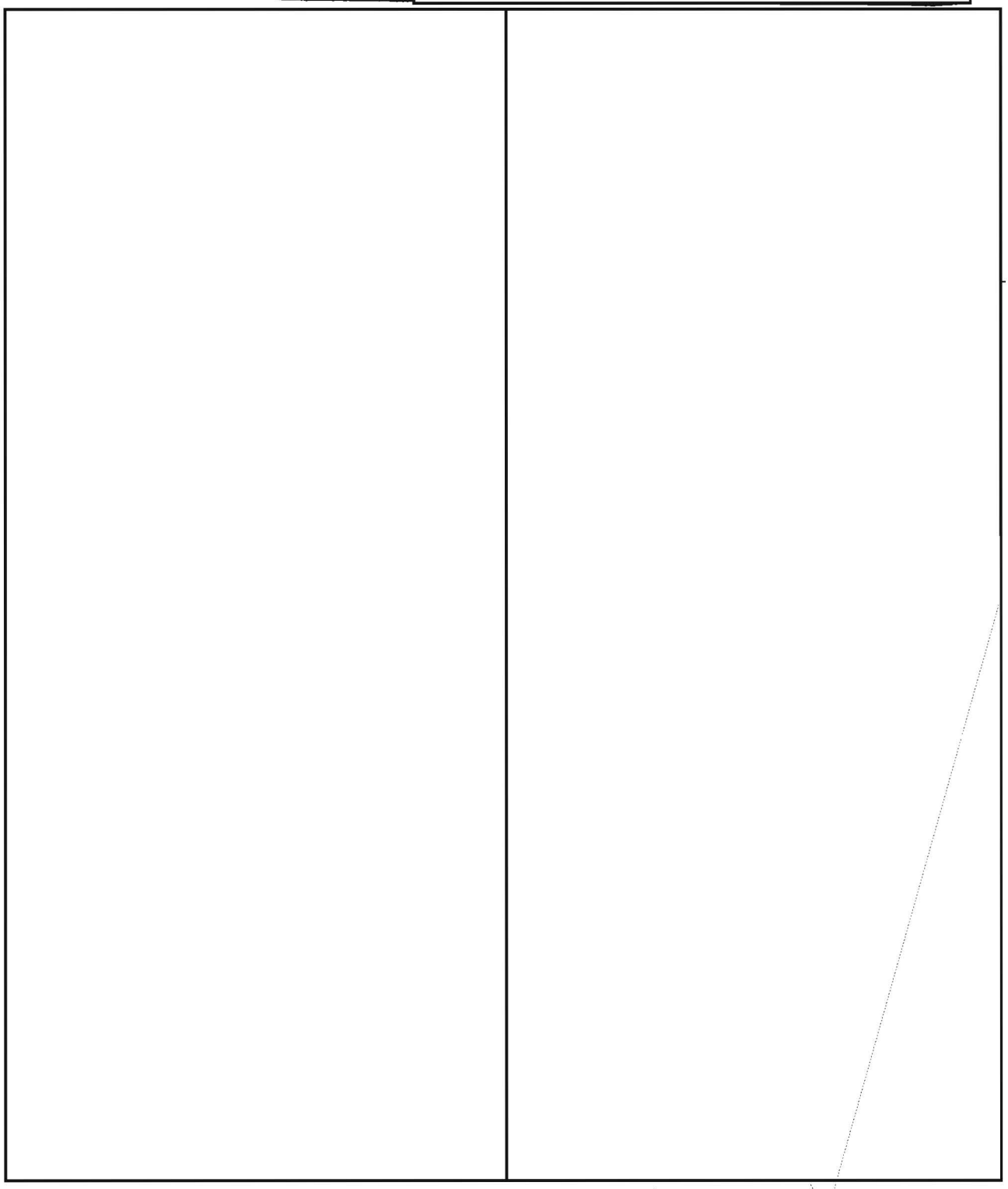
Subsequent sessions, by the group method, involve a discussion concerning progress, questions and answers, and group hypnosis. But in these group sessions, use is made of the same suggestions on relaxation, concentration, etc. which were outlined above. It's that uncomplicated!

But let me make it clear that hypnosis is not a cure-all. It is not a way of life or a religion, but simply a way to take advantage of unused mental capabilities. It can do a lot of things but it cannot *cure* anything, and it cannot make you do anything unless you want to do it. So if you really want to learn a language but are having problems speaking it, or memorizing words or grammatical forms, hypnotism is just one way of getting help. Why not try it? Just relax. . .

~~CONFIDENTIAL~~

WAVEGUIDE ANALYSIS

P.L. 86-36



P.L. 86-36

~~CONFIDENTIAL~~

A SIMPLE CIPHER STORY

William P. Meyer,
C512F

Many years ago, having read Edgar Allan Poe's "The Gold Bug" and articles on codes and ciphers in the old *Shadow* magazine, I thought it would be a simple matter to construct a cipher to keep private some love letters I had received during my high school days. I knew my wife-to-be would not take kindly to my keeping them even for sentimental reasons.

I thought I had it made by taking the alphabet and cutting it in half. Since I knew what the message said, I would find it a simple matter to substitute the correct letter in case of doubt. The cipher was similar to this:

ETAIONSHRULDM CBGVFPJYWKXZQ
QZXKWYJPFVGBC QZXKWYJPFVGBC

In other words, I reversed the last thirteen letters and repeated them twice.

I immediately enciphered the letters, keeping the same format, and threw the originals away.

Dear Bill, (Clear)
BQXF ZKGG, (Enciphered)
DEAR TILL, } (Two possible solutions)
ZCGW BVXX, }

x x x x Body of the letter x x x x x x x x

(Clear)	Love, Virginia
(Enciphered)	GWKQ, KKFXKYKX
(Two possible solutions)	LOIE, IIRAINIA XFVC, VVWGVPVG

Needless to say, about three months later my wife presented me with the letters, neatly deciphered. She was wondering why I thought they were worth keeping.

Now the romantic thing for me to have done would have been to join the Foreign Legion, but since I was patriotic, I joined the Army. I was sent to Fort Monmouth, New Jersey, attended the U.S. Army Signal Corps School, and graduated as a Cryptological Technician, MOS 805.

It is true that, in this day and age, the romantic notion of keeping love letters, either in the clear or enciphered, is no longer the "in" thing. But my advice, born from personal experience and reinforced by practical experience, is:

Always place the externals of your message internally within the body of the message.

(UNCLASSIFIED)

GEOGRAPHIC NOTE

(Continued from p. 4)

in 1920, and then was renamed *Liepaya* after Soviet incorporation.

The back-and-forth naming and renaming of places in the Baltic area is not a unique situation. Throughout the world, placenames are constantly changing. Old cities are given new names. New cities are being created. Countries whose names we remember from postage-stamp collecting years ago still exist, but with different names. So if, in your work, you encounter any difficulties with placenames, of any vintage, check with the NSA Geography and Map Library, C525, extension 5725 or 5726. We're here to tell you where it's at.

[redacted] C525

(UNCLASSIFIED)

CLA ANNUAL BANQUET
Thursday, 27 May 1976.
Trojan Horse Restaurant,
Holiday Inn, Silver Spring.

Speaker: [redacted] (formerly ONI & CIA; now retired): "Elegant English"

For information, call: Banquet Chairman, [redacted] x7222s

This issue marks the end of my year's apprenticeship as "the new boy." I hope that, during this year, CRYPTOLOG has had at least a few informative articles of interest to each of its more than 2500 recipients. During this year I have actually heard a few comments, ranging from "That last issue was the best one yet, Art!" to "That last issue was absolutely nothing! -- the worst excuse for a magazine I've ever seen!" (usually said about the same issue). I've enjoyed editing CRYPTOLOG, even though I have to sniff an awful lot of rubber cement to get the copy into a form that satisfies everyone -- the author, the editorial board, the casual prepublication nitpickers, and, ultimately, the intended reader. The one thing I regret is that I don't have enough time to sniff out ideas for articles and to help authors to develop them. True, I have developed the previous editrix's habit of butting into every technical conversation and asking, "Have you thought of writing that up for CRYPTOLOG?" All a person has to do is burp and I suggest, "Hey, an article on the incidence of gastritis among NSA-ers?" Usually, however, these ideas come to naught. I have a fairly long list of names of people who swore long ago that they would submit an article, but haven't (my "Promises, promises" list).

In the meantime, as I read through the submitted articles, and/or edit them, and/or type them up, and/or paste them up into final copy, and/or illustrate them (you just can't get good help nowadays), I often end up with lots of scraps of paper all over my desk, but also with scraps of ideas for what I think might be good articles. Who can write them, though? I would hate to write them all myself, signing them with noms de plume like "Paul E. Glott." I would also hate to throw the scraps away, just as a person who does a lot of home sewing hates to throw away his best remnants (the libbers have me so confused with "his" and "her," I'm never sure, as an editor, when I'm getting it right). Maybe I can turn these scraps into a "crazy-quilt" end-of-year report. . .

Transliteration

One article I'd like to get from an NSA-er would deal with transliteration and the tricks it plays. An article recently published in CRYPTOLOG mentioned the problems the author had had in locating a certain word in Russian dictionaries. Then, she said in her original manuscript, "COB" jumped off the page and suggested another linguistic tack to take. Since she had been writing about Russian all along, I figured that I'd better ask her which **СОВ** she meant -- the abbreviation for **советский** ("Soviet") or **совершенно** ("completely," "top" as in **совсекретно** "top secret"). When I phoned her, she said, "Neither! It's English! C-O-B -- 'close of business.'" My theory is that when the word jumped off the page, she might have *thought* she was reading English, but I'll bet that it really registered subconsciously as a Russian abbreviation that sent her off on the right trail. "An article on psycholinguistics?"

Jane-Aceisms

Everyone in my generation has a favorite expression as used by Jane Ace on radio aeons ago. With some it's "He's got all the earmuffs of a hardened criminal." With others it's "She's been galvanizing all over town." One of my special treats as editor is to collect the new generation's Jane-Aceisms. (True, I get plenty of them from my own kids, such as "in this day of age," but I can always appreciate more.) Some of them I edit out (for example, in a serious article I changed "tinge of pride" to "twinge of pride," until it dawned on me that that wouldn't do, because a twinge is supposed to make you say "Ouch!") But others I leave in, especially in letters to the editor. I don't do that to be mean (after all, I *do* correct the spelling and change the punctuation in some letters). It's just that a letter to the editor should express the writer's exact words. So what if the writer accuses the editor of "leading field personnel down a primrose path"? Why change it? Why add a snippy "editor's note" pointing out that people lead *other* people "down the garden path," but people (at least the ones I know) usually take "the primrose path" of their own volition? No, whether I edit them out or leave them in, I just enjoy these "almost-right" expressions. I only wish that someone would write an article about them -- maybe "Jane-Aceisms at NSA"? I'd

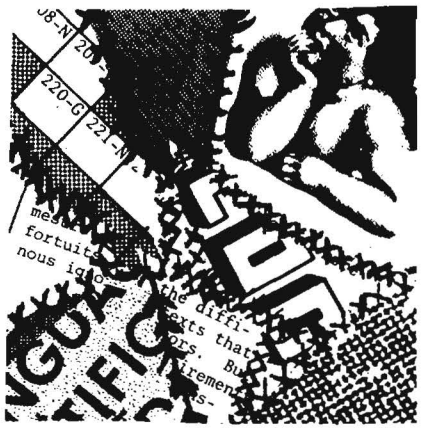
give the author all my best examples, including the one I heard in the cafeteria a few weeks ago. Three guys playing cribbage. One almost wins the game. One of the others says, "Close, but no car!" If anyone volunteers to write the article, I'll promise to find a picture to illustrate it -- an angel wearing black shoes. And I'd give him all the stores that former NSA-er [redacted] told me about his chief petty officer, including the story about the time that all hands were supposed to show up for inspection. One of the men (he's always named Kozlowski in stories like this) was wearing white socks with black shoes. The petty officer said, "Kozlowski, you will go BACK to your area! You will REMOVE them white socks! You will report back here wearing BLACK socks with black shoes! And in the HEREAFTER, you will wear black socks with black shoes!"

Geographical names

I've always liked geographical names. In fact, I first got interested in Russian when, during World War II days at Fort Lewis, Washington, I would have to stand, several times a day, either alone or with one or more other enlisted men and stare, while otherwise engaged, at a map of the USSR that was posted on the wall. I guess that the official feeling was, "As long as they're going to be standing there anyway, they might as well learn Rooski geography!" At any rate, I find geographical names absorbing and always try to get them right in CRYPTOLOG articles. "Da Nang" versus "Danang" was an easy one. But the names in an article in this month's issue were particularly tough -- places that had had German, Latvian or Estonian, then Soviet names (including names "not recognized" by the U.S. State Department), renamed Soviet cities, etc. The problem represented by Libau-Libava-Liepaya is a common one in Eastern Europe. I remember an emigré who had come from L'vov (in the Soviet Ukraine, but at one time Polish Lwów or German Lemberg). His grandfather insisted on calling the city Lemberg. So did the grandson until, one day, there was a showdown in school. The teacher said, "Pupil Ivanov will stand up!" He did so. "Pupil will come to front of room!" Did so. "Pupil will face class!" Did so. "And now -- pupil will say we're in L'vov!"

NSA-Crostics and other frills

Don't look for the definition "What the teacher told pupil Ivanov in L'vov (formerly Lemberg). . ." when doing the next NSA-Crostic. But look for a similar one. Because it seems that, despite all the erudition that is crammed into these once-every-three-months puzzles, the only things that seem to register on the readers, according to comments I hear, are items such as "Wait till the nun signs, Shelly!" Which brings me to other frills -- the illustrations in CRYPTOLOG. Some people think that CRYPTOLOG should have no illustrations at all. They feel that if an article on submarine warfare is illustrated with a pussycat staring at a goldfish bowl, the only thing that people will comment on is the damned pussycat -- they won't even bother to read the article. But another view is that the illustrations are supposed to lure people into reading articles that they would normally leave unread. Or to jog their memory months later -- "Yes, I remember reading an article on submarine warfare in CRYPTOLOG -- or was it the Tech Journal? -- it had a picture of a pussycat staring at a goldfish bowl!" Which opinion do you share? More illustrations? Fewer? More articles on a certain subject? Fewer? Please make your feelings known to any one of the members of the Editorial Board, so that we can take them into consideration in future issues. Incidentally, if you're in favor of *more* articles on a certain subject, why don't you write one of them?



Letter to the Editor

To the Editor, CRYPTOLOG:

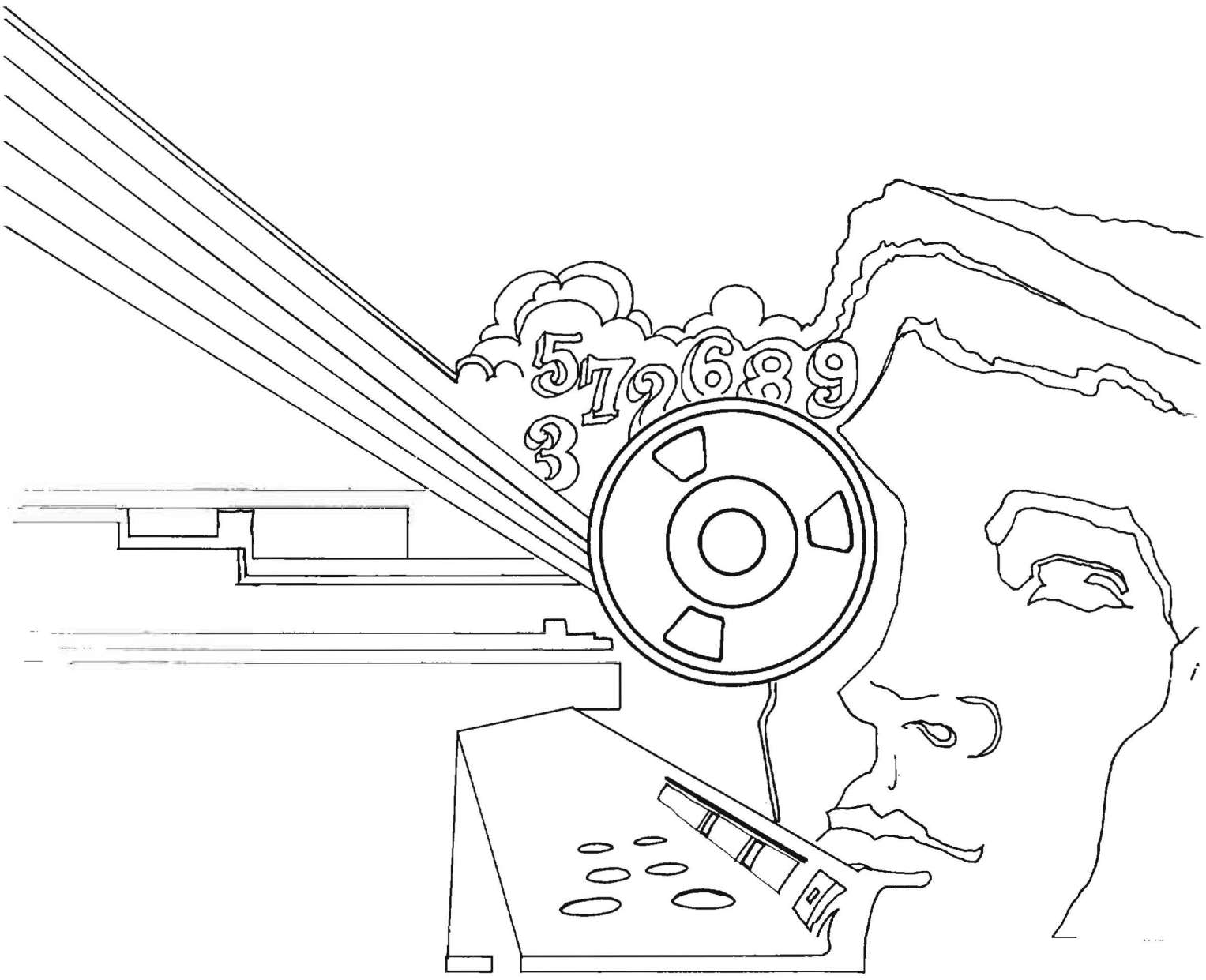
I greatly enjoyed [redacted] *article on Soviet slang in the February issue. But what does that drawing at the end of the article represent?*

[redacted]

Editor's reply:

The drawing didn't come out too well (when the master plates were reduced 20% in printing, the table came out too dark). It's supposed to be a little old lady's desk. She has removed her spectacles and has put down her magnifying glass. She had been using the magnifying glass to check the cut-out Russian words in her dictionaries. Visible in the magnifying glass is the end of one word: ---HO. Incidentally, your last name isn't in the phone book, but it's in Webster's. Are you sure your name isn't [redacted]

(UNCLASSIFIED)


5 7 2 6 8 9
3