

Declassified and Approved for Release by NSA on 10-11-2012 pursuant to E.O. 13526, MDR Case # 54778

mified by DIRNSA/CHCSS (NSA/CSSM 123-2) - Exempt from GDS, EO 11652, Category 2

sify Upon Notification by the Originate

THIS DOCUMENT CONTAINS CODEWORD MATERIAL

TOP SECRET

P.L. 86-36

DOCID: 4009793

-TOP SECRET

EGYPTOLOE

Published Monthly by Pl, Techniques and Standards,

for the Personnel of Operations

VOL.	IV,	No.	4			APRIL	1977

PUBLISHER

WILLIAM LUTWINIAK

BOARD OF EDITORS

litor in ChiefArthur J. Salemme (5642s)
DilectionP.L. 86-36
ryptanalysis
anguageEmery W. Tetrault (5236s)
achine Support
athematicsReed Dawson (3957s)
pecial ResearchVera R. Filby (7119s)
raffic AnalysisFrederic O. Mason, Jr. (4142s)
roduction ManagerHarry Goff (4998s)

For individual subscriptions send <u>name and organizational designator</u> to: CRYPTOLOG, P1

TOP SECRET

UNCLASSIFIED



During the last year or so, a number of scientific writers have published articles discussing cyclical recurrences of world ice ages, including the possibility of future recurrences. If the winter of 1976-1977 in the greater Washington-Baltimore area is any indicator, the next "cycle" could now be in its formative stage! As this article is being written (early January 1977), the Washington temperature is 13° F., and the chill factor is below zero.

Sometimes we do not appreciate that the Russians, as a whole population, have always lived with wind, ice, snow, fog, and extremely low temperatures throughout a great part of their country, all their lives, and through many generations of Russian peoples. By necessity they have learned to

adjust to these severe climatic conditions. The important industrial and port city of Murmansk, for example, has 200,000 inhabitants living and working there year round (and the "greater Murmansk area" --Murmansk Oblast -- has one million year-round inhabitants). Murmansk itself is located above the Arctic Circle, on the Kola Peninsula. at about 69° north latitude. It is hard for many people to realize that almost all of the state of Alaska is situated south of that latitude. The Soviet Union's largest and most potent fleet -the Northern Fleet -- is headquartered near Murmansk at Severomorsk, and most of its ships operate from home bases located in and around the Kola Peninsula.

Fortunately for the Soviet Navy, the North Atlantic Drift, i.e. the northern reach of the famed Gulf Stream, finds its eventual terminus hard against the Kola coast. By the time it reaches those extreme latitudes, it carries

just enough warmth to keep the southern Barents Sea relatively ice-free year round. Even so, the less mobile and less-warmed estuaries and riverine outflows freeze in the winter and have to be kept open through the continuous use of icebreakers. The Soviet Navy and merchant fleet rely heavily on icebreakers, including the new nuclear-powered ARKTIK-class supericebreaker of 25,000 tons standard displacement. There are 45 icebreakers in the Soviet maritime service, more such units than of any other service-force type found in the Soviet Navy. (Submarine tenders are in second place.) Viewed in the naval context, icebreakers in the Soviet Union account for over 30 percent of the aggregate tonnage of the naval service force and for just over 9 percent of the aggregate displacement of the entire Soviet Navy.

Prevailing winds across almost the whole of the Soviet Union emanate from the north and northwest in July and from the south and southwest in January. Highest actual temperatures in July do not, for the most part, exceed 70° F., and, in January, drop to from -30° to $+30^{\circ}$ F. Permafrost (perennially frozen ground) occurs extensively in the USSR. This creates extremely adverse financial and technical problems for development: small gains can be made only at great costs. Agriculture is negligible in such areas: there is little or no growing season. Most food supplies, as well as almost all manufactured goods must be imported. Any heat leaking from road surfaces or structures leads to flooding and soil subsidence, with considerable structural damage. Accordingly, public works and human habitability systems require special, costly engineering and cold-weather maintenance.

April 77 * CRYPTOLOG * Page 1

P.L. 86-36

UNCLASSIFIED

All of the Soviet Union is affected by only three seasonal climates:

- 80 percent of the country experiences
- cool summers and cold winters,Another 10 percent experiences a full
- summer and a cold winter, and
- The remaining 10 percent sees only a very short and very cool summer, followed by a very long and very cold winter.

Above 58° (latitude of Labrador) lies nearly half the USSR, where the soil is predominantly the high-latitude *podsols* (soils with acidic, nearly structureless upper layers) or the *andept inceptisols* (soils which contain high amounts of clay, are perennially or seasonally wet, and have little or no horizons of redistributed materials). These soil types are found on high-latitude wastelands, tundra, and ice caps, and millions of acres of coniferous forest, all of which areas are tractless and without access or inhabitation.

Given these adverse conditions, one sees the climatological sense of what appears to be a certain Russian predilection for cruises to warm-water ports, continous naval deployments in the Mediterranean Sea and the Indian Ocean, and sometime voyages to the Caribbean Sea, Philippine Sea, Middle and South Atlantic Oceans, and elsewhere below 40° north latitude. Such rangings of the Soviet Navy and merchant fleet should not be viewed with exclusive respect to their more obvious political, military, and economic dimensions. It does not seem altogether facetious to regard Soviet maritime expansion in a climatic and physiographic light.

Consider, if only momentarily, the possible consequences for international security (that is, NATO) and U. S. national security of a gradually advancing future "ice age." (Here, there is neither the space nor the rationale to debate the merits of some of the climatologists' arguments.) Assume only that there will be another ice age in the imaginable future. With what increasing covetousness might the Soviets come to regard seaports and habitations below 50° north latitude? On the land, the Middle East, Africa, and South Asia could prove increasingly attractive. A place like Angola with a relatively small native population and an extremely large supply of largely undeveloped minerals and arable soils, seems properly worth a substantial commitment. In 1973, Angola already had the fourth-highest gross national product per capita of the approximately 50 African countries, and produced, on a largely undeveloped basis, 750 to 1220 calories per person per day. As early as 1963-1965, iron-ore production at Cuina and Cassinga was large enough to be listed in world economic atlases. Mackerel, sardines, and anchovies inhabit the waters off Angola, Gabon, and southwest Africa. The port of Luanda is well developed for general (dry) cargo transfer; the USSR merchant fleet is heavily

specified in general (dry) cargo bottoms. In the Congo, immediately north of Angola, at Tchitondi, is located a fertilizer center which was able, in 1969, to produce 100,000-500,000 metric tons of phosphates annually.

One more point needs to be stated: If there is to be another slowly encroaching "ice age" (and the purpose of this article is not to take one position or another on that question), then the Soviets probably are, or will be, better informed on that subject than any other people in the world. Only Scandinavians, and North Americans -- although in nowhere near the numbers of Russians -- generally live in the high northern latitudes. Continuous Russian polarresearch programs predate the October 1917 revolution. The continent of Antarctica was discovered in December 1817 by a Russian naval officer, one Lieutenant Thaddeus von Bellingshausen*, whose voyage, emanating from the Baltic Sea, was specifically tasked to see in what the "other" polar region consisted. Insofar as Soviet nonmilitary technology and research are highly developed, they are most highly developed in arctic-polar matters and in the transportation, exploitation, and industrialized habitation of the extreme latitudes. Their prior commitment to developing such potential as exists in those reaches of geography is driven by historical, geographical, and demographic necessity. On balance, the Russians probably stand to suffer more from a future ice age than do Scandinavians or North Americans . or Chileans and Argentinians. The thesis of this brief discussion is merely that an advancing northern ice cap, pushing in its path the great ice pack, may have long-range implications for Soviet political, economic, and military expansion -- or may, even now, be a valid consideration not only in the United States and among its allies, but also certainly in the Soviet Union, where much of the cold-weather existence is experimental and delicate and from whence the only direction to move under insurmountable pressure is south.

<u>*Editor's note</u>: One reason why Antarctica has international status is because a lot of countries claimed to have "discovered" it around that time, including the United States, on the basis of the official log of an 18-yearold whaling captain from Stonington, Connecticut, whose crew had actually disembarked onto the continent and were cavoring around when they heard strange bells coming through the fog. Turns out it was Bellingshausen's ship, and the Russians had a good laugh out of it, saying, "Here we thought we had discovered a continent, even though we haven't seen it yet, and now we see that a young-punk American has beaten us to it!"

╡_╋╔╗┍╗╔╗╔╗╔╗╝╗╝╗╝╗╝╗╝╗╝╗╝

April 77 * CRYPTOLOG * Page 2

UNCLASSIFIED

DOCID: 4009793

TOP SECRET UMBRA

"IT'S GOT TO GET OUT TODAY!" In January 1977 Frances Blank retired from the Agency after a long and distinguished career. One indicator of her high professional standards is her having won, jointly with the first Frances the first (1973) Sydney Jaffe Award for Outstanding Contri-Blank, butions to the Language Effort at NSA. Shortly P.L. 86-36 G52 before her retirement, Ms. Blank spoke to the CLA's Special Interest Group on Translation, giving much practical advice based on her operational assignments. The following article is a slightly expanded version of that talk. ${f B}$ efore any discussion of my ideas on transif I were pinned down, I would come near to agreelation of end product, a word of warning may ment. I question only the "all" part of it. not be out of place. I have frequently been Accuracy is important, but it has to be told, when I expressed disapproval or amazement considered constantly in relation to timeat certain procedures in other linguistic areas, liness. "But you don't understand! You've always been Timelinessin an old-line section. You don't know what it's like in other places." This charge is undoubtedly true, but since my views were formed and are colored by by own experiences, I cannot ignore them in discussing translation. As for languages, my experience has been largely in Romance, with some Germanic. Moreover, I have worked an unusually high proportion of flaps, swing and graveyard shifts, and holidays. For several years, Saturday or Sunday, or both, have been part of my regular work week. Indeed, the title of this article came to me one Saturday when I was trying to find care! It's got to go out today!" NSA translation, it has always seemed to me, is marked by three qualities: timeliness, accuracy, • style. I have listed these qualities in what I consider to be their order of importance. I am aware that there are many Agency linguists who would shout out, in outraged chorus, "No! In our work, accuracy is all-important!" Actually, April 77 * CRYPTOLOG * Page 3 EO 1.4.(c) TOP SECRET UMBRA.L. 86-36

EO 1.4.(c) DOCID: **4009793**

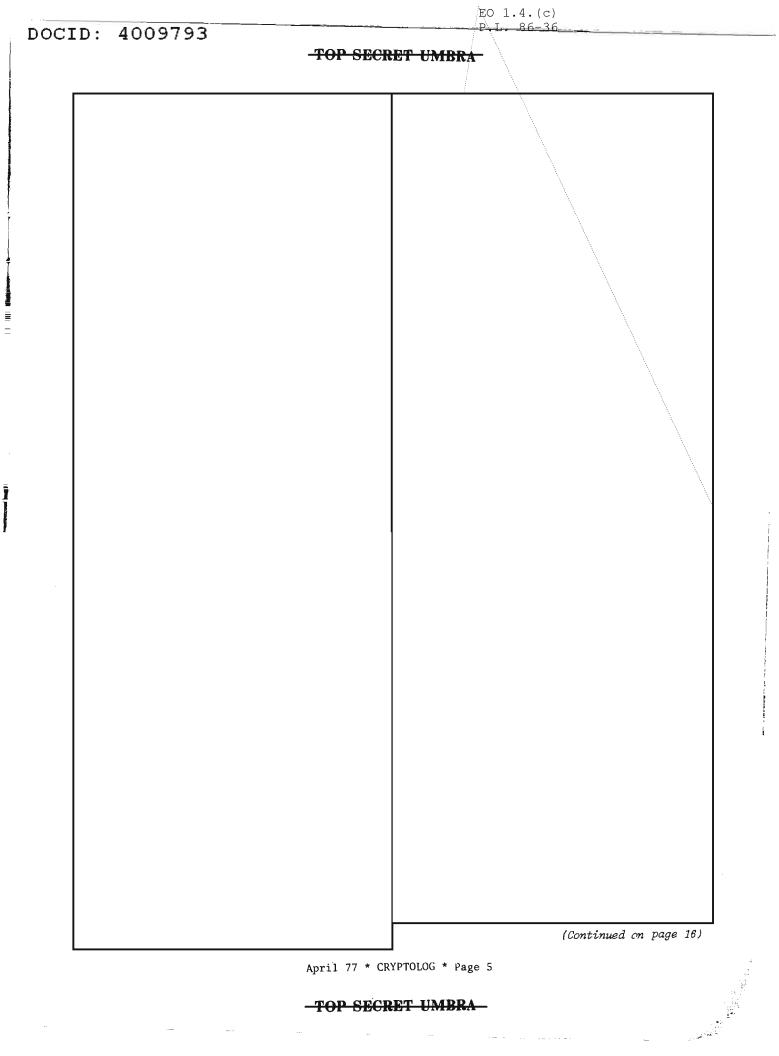
TOP SECRET UMBRA

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

Anyone named Blank understands about sensitivity to names. In fact, when Hecht's first installed its computers and elected to call me Frangert Blank, I protested by letter the first month. Then I marched down to Hecht's the next month and told the lady in Complaints that, much as I valued my Hecht's charge account, I was going to have to cancel it because my ulcer simply would not endure facing Frangert every month. Fortunately, she had a sense of humor.	
	And what about abbreviations? The transla- tor is instructed to expand them. Yet BP, KLM, and BMW are better known than their expansions. And how many people can expand fob, rif, or even a.m. and p.m.? TV hasn't quite reached that point now, but I suspect that in another generation there will be people who do not know the expansion for TV. In the same way, many abbreviations in the traffic, quite exotic to the translator, are old friends to the real customer. Certainly expand them if you can, but do not delay publication, or waste time looking for them. Your customer will know.

April 77 * CRYPTOLOG * Page 4

TOP SECRET



-TOP SECRET UMBRA

UNCLASSIFIED

12345

205

P.L. 86-36

W16



5,704,689,200,685,129,054,721

x 59,649,589,127,497,217.

To place this in perspective, let us see what would be involved if we simply approached this problem without an algorithm and tried to work our way up to the smallest factor, starting with 1. There are 31,556,952,000,000 microseconds in our year -- a 14-digit number. Assuming that, in our search for the smaller factor above -- a 17-digit number -- we use a computer capable of performing one operation per microsecond, it

could require about 2000 years of our machine time to find this number. By the way, this is not simply an exercise for the fun of it. The factors of $2^{128} + 1$ are of use in designing codes for space communications, and the same type of considerations arise today in carrying out some of NSA's challenging communication tasks.

This capability has arrived during the lifetime of most of us, for the first electronic computer was the University of Pennsylvania's ENIAC, operational in 1946. One might contemplate the implications of the rapid increase in computer speed. The adding speeds for 10-digit numbers are of the order of the following:

		Additions per <u>second</u>
19th, early 20th century	mechanical calculator	4
1960s	medium-speed computer	200,000
today	high-speed computer	200,000,000

Knuth (D. E. Knuth, *Science*, <u>194</u>, No. 4271, 1236, 1976) compares this acceleration to that of transportation speeds:

	<u>Miles per hour</u>
snail	0.006
man walking	4
U.S. automobile	55
commercial jet plane	600

Even if we add a nominal near-earth satellite, with a speed of 17,400 miles per hour, the ratio of the computation speed of today's computer to mechanical calculator is approximately 11,500 times greater than the speed of our satellite compared to a man walking. When one notes the cultural impact the transportation-speed increase has had on mankind, can one help but wonder what the computer impact ultimately will be?

April 77 * CRYPTOLOG * Page 6

UNCLASSIFIED

Computer listings and "IBM cards" are such commonplace items in our lives here at NSA that most of us probably take for granted the rather awesome capability that lies within the Agency's high-speed digital processors. Similarly, many of us probably take for granted the computer power that is readily accessible to anyone who can afford even the simplest pocket calculator.

MICON

83810205

It was not too long ago that the type of calculation that we perform today in fractions of a second had to be done by hand with the aid of logarithm tables. The very tediousness of the operations prevented many problems from being considered. Today, using high-speed computers in combination with mathematical techniques the principles of many of which have been known for a century or more, we are able to perform operations that would have been unbelievable to a nineteenth-century mathematician.

For example, recently Morrison and Brillhart (M. A. Morrison and J. Brillhart, *Math. Comput.* 29, 183, 1975) tackled the problem of discovering the prime factors of $2^{128} + 1$. This is the 39-digit number:

340,282,366,920,938,463,463,374,607,431,768,211,457.

Their answer, determined after about 1 1/2 hours of computer time, is:

74,607,431,768,211,457.

Another aspect for contemplation is our growing dependence on computers and calculators In our division, if the computers are down, so is our productivity. This dependence was strikingly called to my attention on a recent airplane flight where two individuals seated next to me were assembling cost figures on their week's sales efforts. When it came time to add up the column of figures, they discovered their pocket calculator was discharged. One then told the other, "I no longer trust myself in adding figures like this since I have grown so used to using my calculator." They put their work away without the final sum.

It was not too long ago that agility in mental arithmetic was widespread. This was particularly true of astronomers, who had numerous dreary calculations to perform. One very wellknown American Astronomer who possessed a remarkable mental calculating ability was Truman Henry Safford (1836-1901). Ashbrook (J. Ashbrook, *Sky and Telescope*, November 1976, p. 346) has uncovered some documentation, which there is no evident reason to doubt, illustrating Safford's talents. I repeat several of the anecdotes here.

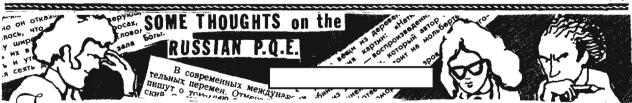
A friend gave Safford the following problem: "Suppose I was born at a certain hour, minute, and second of a certain day of a certain year (where the friend supplied values for the certain), how old would I be, in seconds, at noon today? Safford walked up and down along a blackboard and told him the answer. The friend responded, "No, that is not correct, for I have worked it out and the answer is different." "What was your answer?" asked Safford. When he was told, he retraced his path along the blackboard and then exclaimed, "Oh, you forgot the leap years." Safford was right.

Safford's ability was recognized by the time he was 9 years old. An interviewer asked him, "How many acres are in a circular piece of ground with a circumference of 31.416 miles?" The child flew around the room and in a minute answered, "50,265.6." He was next asked, "What is the entire surface of a regular pyramid whose slant height is 17 feet, the base a pentagon of which each side is 33.5 feet?" In about 2 minutes he replied, "3,354.5538." He could routinely take a column of about 40 numbers with from two to four figures in each number, and in about 5 seconds write down the sum of the squares of these numbers.

Perhaps the most astounding feat was when he was asked to square 365,365,365,365,365,365. It is reported that in less than a minute he gave the answer from left to right:

133,491,850,208,566,925,016,658,299,941,583,225.

It took me considerably more time than this to verify the answer using the calculating tools I have available from my desk. If anyone reading this can do this type of calculations in his or her head, we could use you when the computers go down!



Jhe Russian Professional Qualification Examination (PQE) is a topic guaranteed to stimulate lively discussion among NSA's Russian linguists. And if you want to get into a really heated conversation, spend an hour or so with an aspirant who has failed a portion of the PQE more than once -- he will have a definite opinion on what can be done with the PQE. The frustration, despair, and anger of such an aspirant are understandable for, it seems to/him, his career advancement and promotion are inseparably linked with passing the test. To some, particularly those who have been with NSA for only a few years. the PQE becomes the added frustration that makes working at NSA almost unbearable. Unfortunately (perhaps fortunately in some cases), some linguists eventually/begin boycotting the tests; others seek job reclassification to pursue a career elsewhere. The loser in such cases is NSA because, usually, large investments in time and money have been made to train the aspirant to become what he will not be if he abandons the language career field.

P.L. 86-36

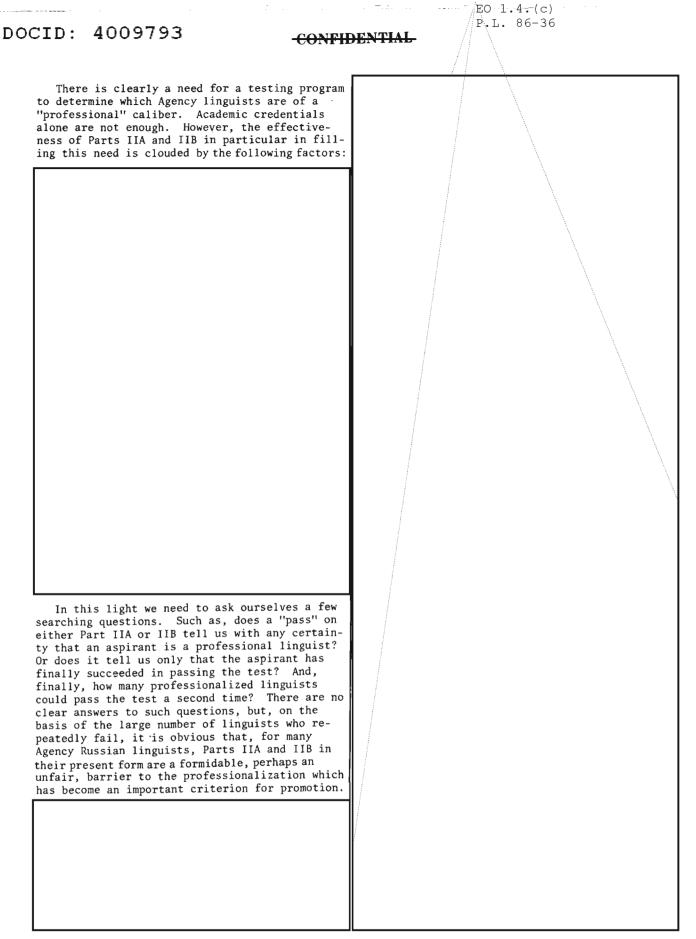
For this reason, and because language professionalization is a particularly timely topic, I would like to share with CRYPTOLOG readers a sampling of the opinions expressed by discouraged aspirants. Some expressed feelings which are no more than vague complaints about the "unfairness" and "irrelevancy" of the PQE; others have voiced more compelling evaluations and arguments. It is my intention here to note only those valid and reasonable complaints which are, in my opinion, worthy of the Language Career Panel's consideration. The audience I have in mind is those Agency linguists who are receptive to criticism and who are in a position to effect meaningful changes in PQE policy. I also wish to address the aspirants, those who are finding it difficult to pass all parts of the PQE, and those who will soon be taking the tests for the first time, to ask for their forbearance as well as their suggestions, and to reassure them that the "testmakers" are aware of their frustration and are striving to devise better tests.

(CONFIDENTIAL - CCO)

April 77 * CRYPTOLOG * Page 7

CONFIDENTIAL

HANDLE VIA COMINT CHANNELS ONLY



April 77 * CRYPTOLOG * Page 8 :

CONFIDENTIAL

CID: 4009/93	CONFIDENTIAL	E0 1.4.(c) P.L. 86-36
	CONFIDENTIAL	
		•
	April 77 * CRYPTOLOG * Page 9	
	-CONFIDENTIAL -HANE	DLE VIA COMINT CHANNELS ONLY

UNCLASSIFIED

NSA-crostic No.7

The following NSA-crostic was submitted by guest NSA-crostician L. R. Chauvenet, P12.

DEFINITIONS

- A. Caesar's mother
- B. Reflector
- C. Deep dish fruit pie
- D. If two do it, it may make a to-do (3 wds)
- E. Ready
- F. Eager
- G. A Vermont answer to the question, "Have you lived here all your life?" (2 wds)
- H. Part of a ton
- I. An opinion of the paleface
- J. What the sign carried by the tackle said (4 wds)
- K. How a burden might feel to a left-handed man (2 wds)
- L. You can do this with flowers
- M. Concentrated quarters of a racial minority
- N. We sometimes hope retirement will bring us a life of this
- 0. Yellow green
- P. Lacking nourishment
- Q. A call to dinner which made the Frenchman suspicious (2 wds)
- R. A branch of philosophy
- S. "Would she could make of me a saint, or I of her a -----"
- T. Common meeting place
- U. What the prisoner said when the judge shouted, "Order in the court!" (4 wds)
- V. Matter in a state

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

	W	ORDS									
66	15	146	120	89							
141	105	37	134	71	7						
139	34	75	111	64	162	171					
82	145	5	80	165	1	55	127	123			
59	84	112	167	21	142	50	106				
47	104	154	181							`	
149	178	113	65	110	3						
148	119	46	99	73							
164	137	14									
17	175	31	4	138	87	158	96	72	36	151	41
118	70	163	10	129	100	6	53	157	176		
61	126	29	156	102	169	52					
13	115	38	69	77	28						
143	63	116	131								
93	54	11	153	135							
85	12	170	103	51							
155	2	92	88	24	81	173					
25	177	9	79	107	33	101	174	152			
44	26	168	108	57	23						
109	42	124	117	67	58						
160	130	95	97	18	180	60	8	20			,
40	147	91	98	136	30						

April 77 * CRYPTOLOG * Page 10

UNCLASSIFIED

DOCID: 4009793

UNCLASSIFIED

- W. Confuse
- X. Water conservation expedient (3 wds)
- Y. Why my picture might have made it seem I was twins (3 wds)
- Z. Proprietor

ŝ

Z₁. What you might do to alleviate the condition of Word P (2 wds) 39 83 74 166 172

78 179 48 132 45 62 144 121 90

- 86 56 43 159 114 150 140
- <u>133 94 27 125 32</u>

<u>68 122 19 161 49 22 35 76 128 16</u>

1 D	2 Q	3	G	1		- *	4 .	J	5 [)	6	K	7 1	В	8 I	J	9 F	٤	10	K	11	0	12	Р	13	М	þ		14	I
15 A	16 Z	_			17	J	18	U		***	19	Z ₁	20	Ū			21	Ē	22	Zı	23	Ś			24	0	25	R		
									•																					
26 S												J																	37	
38 M	39 W	4	0	V		·	41	J	42	T	43	Ŷ	44	S	45	X	46	H	47	F	48	X	49	Z1	50	E			51	Р
52 L	53 K						ļ																						65	G
	66 A	ł				-			1						1														78	Х
79 R																														
91 V	92 Q	9	3 (0	•		94	Ż	95	Ū	96	J			97	U	98	V	99	Н	100) K			10	I R	102	L		
103 P																														
	117 '	T 1	18	K	119	H	120) A			12	1 X	122	2 Z1	12:	3 D	124	T	125	Z	126	ί			12:	7 D	128	Z1		
129 K	130	U 1	31	N			132	2 X	133	δZ	134	4 B	135	5 0	136	5 V	137	I	138	J			139	C	14() Y	141	B	142	E
143 N		1																												
156 L		1 ; ;	57	K	158	J	159	Ŷ			160	D U			161	Z1	162	<u>2</u> C	163	K	164	I	165	D	160	5 W	167	E	168	S
169 L		1	70	P	171	С	172	Ŵ	173	Q	174	4 R	175	ξĴ	176	δK			177	R	178	G	179	X	18() U	181		L.R	.C.

April 77 * CRYPTOLOG * Page 11

UNCLASSIFIED

(Solution next month.)

THE LAST WORD ON LATS? CECIL PHILLIPS, CO3 - -

Swift/Oliver Aid on Code Reconstruction

The revised edition of *Collected Articles* on *Code Reconstruction**, compiled by Katharine Swift and is now available.

The foreword of the 314-page publication states:

"This collection of articles, most of which have previously appeared in various Agency publications, is a revised version

*Publication of Cryptanalysis Department, National Cryptologic School, 1976. TSC, CCO, S-212802. of a collection edited by Katharine Swift which was published in 1973. A demand for more copies after depletion of the supply has necessitated an early revision.

"While it has not been possible to include all pertinent articles in one publication, it is hoped that managers as well as bookbreakers and programmers, and senior analysts as well as neophytes, will find material that will help each in making his individual contribution on the job.

Anyone with a Top Secret Codeword clearance can obtain a copy of the publication by calling Harry Goff, P16, x4998s.

(F0U0)

Editor"

April 77 * CRYPTOLOG * Page 12 P.L. 86-36

-CONFIDENTIAL

HANDLE VIA COMINT CHANNELS ONLY

FLASH! 115th S.R.I. LOCATED! A. J. Salemme, P16

Now that everyone is writing in to Fred Mason, filling in the gaps in his excellent compilation of radio stations ("Where Were We?", CRYPTOLOG, January-February 1977), it's time for me to add my bit. Where Fred has:

RADIO INTELLIGENCE COMPANIES

111, 112, 125, 126 under Gen MacArthur in SW Pacific	2345?
113, 114, 116, 117, 118, 121, 124 129, 137 in Europe	2345?
115, 119, 120, 122, 123, 127, 130-136, 138 unlocated	2345?

I'd like to add:

115th Sig Rad Int Co, Presidio, S. F. $3_{4,4}$ 115th Sig Rad Int Co, Fort Lewis, Wash. 456

How do I know? Because I was there! And the memories those terse entries evoke!

In the hot summer of 1943, I, a city boy who had never seen a real horse, took my basic training at Fort Riley, Kansas, in what was the last horse-cavalry (the real troopers all called) it the "hoss-calvary") unit in the U. S. Army. They tried to teach me, first of all, to ride a hoss. Rule 1: "Take care of your hoss first." We would ride out to the riding-practice area and ride around in a large circle while the drill instructor in the middle would holler, "I said 'Canter!' Who told you to gallop?" I clearly remember one day when I was on the horse one minute and seated on the ground the next, with no recollection of what must have been the majestic flip that made the transition between the two states. ("Who told you to dismount, trooper?") After practice, we'd go back to the stables, rub down and curry the horses, wipe the horse sweat off the gear and saddlesoap it, clean out the horse's hooves, clean the dock, etc. And then lead the horse to water. Believe me, he would want to drink! But you had to slow him down. ("You kill that hoss with cold water, trooper, and it'll be statement-of-charges for you!") Put the horse back in the stall and then, only then, could you, the trooper, get a drink of water for yourself. And did that vile-smelling Kansas water coming out of a green-encrusted faucet ever taste good! To this day when, watering the lawn on a hot day, I pause to take a gulp of water from the hose, the taste of the brass nozzle takes me back to Fort Riley.

The second thing they taught me at Fort Riley was Morse code. The Army's idea was to send me, along with other city boys (no one I knew who actually yearned to be in the hoss calvary and wear those distinctive jodphurs and high boots actually made it), to a radio reconnaissance outfit. We practiced our Morse code and practiced establishing radio contact. One guy would send while the other cranked a portable hand generator. Then we would break down the equipment, load it onto our two hosses, and move to the next stop. The concept was to send us poor excuses of hossmen and Morse operators -- would you believe? -- *ahead of* our troops on those steamy South Pacific islands, with our hosses crashing quietly through the underbrush, until we detected some Nips, and then get off our hosses, set up business, and start transmitting the news back to base -- one guy cranking, and the other asking, "Is B dah-dit-dit or dit-dit-dah?"

Sure enough, basic training completed, I was sent to a radio recon outfit in San Rafael, California, which, I suppose, was as close as they could get to simulating the South Pacific jungle conditions. When I arrived, it turned out that they didn't even have hosses! They had vehicles (pronounced, invariably, "vee-HICK-les"). So forget the canter and gallop! Now the city boy, who had never driven a car yet (we was pore city folks) had to learn driving while double-clutching on a two-and-a-half-ton half-track. (Drill instructor: "Do not scoff at the two-and-a-half-ton half-track, gentlemen! It is a for-MID-able vee-HICK-le!") We would drive up into the California mountains and establish radio contact. "We don't use Morse code. We just stick in these crystals and talk into the mike. But watch what you say, because they're monitoring us!" I remember once, driving through -- what was it? steam? fog? what? -- on the top of a mountain. Then it dawned on me. "It's a cloud!" City boy had discovered that clouds aren't solid like mashed potatoes -- they're nothing but fog up high.

In driving through the mountains, Rule 1 (replacing "Take care of your hoss first") was "Always remember to close the farmer's gate." We would open the gate, dismount, close the gate, and then drive up paths that a mountain goat would wince at. I'll never forget the time when the driver (not me!) misjudged the width of the path and that massive two-and-a-half-ton hulk slid sideways, finally resting at a 45degree angle against one tightly-drawn strand of barbed-wire fence. If I had been brave enough to lean out the window and pluck that strand, the "Bo-o-o-ing!" would still be reverberating around the world. Were we worried? Sure! That if the barbed-wire strand broke and we tumbled down that ski slope, vee-HICK-le and all, some farmer would be mighty mad. Not only that, but there'd be a little matter of a statement of charges for the half-track. If I remember the physical and fiscal terror of the situation, why don't I remember how we got out?

April 77 * CRYPTOLOG * Page 13

We used to simulate maneuvers. I remember one night, long, long after missing evening chow ("You'll get your chow after you find your way back to base!"), being told, "Okay, Salami! [no one ever did get the name right] Contact base and arrange for rendezvous!" Instead of things like dah-dit-dit vs. dit-dit-dah, I had to worry about things like which crystal to use and what's a beat frequency? Plus those daily-changing codewords for locations. One day CUCUMBER would mean "the firehouse in Petaluma" and SPARROW would mean "City Hall in San Rafael," and the next day they'd be something else. I remember one night (my rebellious gastric juices made me do it!) when, in order to resolve an insoluble rendezvous problem, Radio Operator Salami blatted out in the clear, for all the monitoring operators to hear and record, "Where are we supposed to meet, anyway? Is BETTY BOOP the firehouse in Petaluma or the City Hall in San Rafael?" Not only did I not get to crash a hoss through the South Pacific jungle (did anuone?), but I didn't get to crash a for-MID-able vee-HICK-le through it either. No, within a couple of months of my arrival in signal reconnaissance, I was transferred to signal intelligence. It was obvious, from my having flunked my "response to crisis" test, that I sure needed some.

And so I arrived, in November 1943, at the 115th Signal Radio Intelligence Company, Presidio of San Francisco, California. For 4 or 5 months, World War II was rugged, I mean to tell you! Every time that the Golden Gate Bridge is flashed on television (and that's pretty frequent, even without the opening credits for "Phyllis"), one of my kids will say, "Yeah, Dad, we know, we know! They used to make you put on full field equipment, march to the middle of the bridge, and then run non-stop to the other end!" (End of "War is hell" reminiscence.)

Since I was supposed to know Morse code, it was easy to teach me a few niceties like the Japanese Morse code (Kana syllabary) and abbreviated numerals, and make me a Japanese intercept operator. Okay, then, a week of the new frills and onto the job! That meant driving up to the highest hill in the Presidio to the intercept station (it was called "Fubar," an acronym meaning something like "Fouled up beyond all recognition"), and trying to pick up Japanese Morse signals. Some nights they were mighty sparse. It had something to do with the Heaviside layer -- I couldn't figure it out. A lot of guys would switch instead to local San Francisco stations, listen all night to the Andrews Sisters (". . . with anyone else but me-e-e-e"), and put "NIL HEARD" in their log. That was risky, though, because there was a central control room from which the trick chief could patch into any receiver and hear what you were listening to. He could talk to the intercept operator and help him adjust his signal. Or he could even send

Morse code to him. In fact, he would often do that very thing, in order to dispel his own boredom and to provide training for some Andrews Sisters fan who had twisted his vernier a fraction of a second (they didn't have nanoseconds then) too late. I remember one night when Farley was caught that way. The trick chief started sending, from his control booth, a series of Japanese messages that had been intercepted the night before. Everyone was in on the gag but Farley. We clustered around him, saying, "Hey, everyone! Farley's the only one who's picking up a signal!" Farley would feverishly copy the messages. Occasionally he would say, "Dammit, I missed a group!" Miraculously, the "operator in Tokyo" would repeat that group. "Dammit, he's sending too fast!" Miraculously, the "operator in Tokyo" would slow down. After a couple of hours, Farley was still "copying traffic." The trick chief decided to cut it off by carrying out Farley's every wish in ways that should have made it clear to him that it was all a big hoax. But whatever ridiculous thing he did, or whatever we other guys said, Farley kept "copying traffic." Finally, the trick chief sent a message with an address line reading, not in Japanese Morse code but, unbelievably, in International Morse code, "ATTENTION STUPID AMERICAN FARLEY." Farley jumped up, shouting, "Hey, they're sending this one to the Postmaster General!"

But what if the trick chief didn't enliven the proceedings that way? The nights would really drag as we tried to pick up Tokyo. And how many times can the same joke work? Or the joke of crumbling up a pile of intercept paper and setting it on fire under the hard metal chair of a snoring intercept operator with his hand frozen to the dial as he "searched for a signal"?

If anything went wrong -- such as putting "NIL HEARD" in your log when another operator on the other side of the room heard a signal loud and clear on the same frequency -- you might see your name posted on the "Discrepancy List." I remember one country boy asking, "What does that-there 'discrepancy' mean, anyway?", and a city boy replying, "It means 'you keep up dis-crep-an-see how long you stay in this outfit!'"

In the spring of 1944 the 115th moved to Fort Lewis, Washington, probably because the audibility was better there. And there I stayed, as a Jap intercept operator and, later, as a Jap traffic analyst (my, that was a prestigious jump!) until my discharge in March 1946. I did have a little TDY interlude, however. After I had been a practicing traffic analyst for more than a year, another fellow and I were sent to Vint Hill to take a 2-month course in Introductory Japanese Traffic Analysis. We joined a group of 20 guys just out of basic training, during which they had learned Morse code ("Is B dit-dah-dit-dit or dit-dit-dah-

April 77 * CRYPTOLOG * Page 14

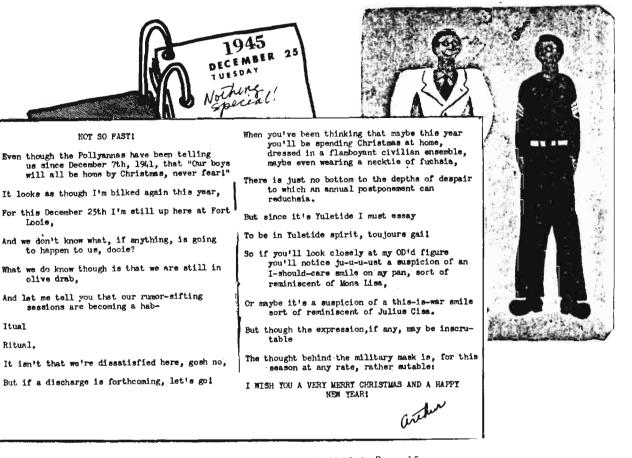
FOR OFFICIAL USE ONLY

dit?"). When, all by myself (the other guy had taken some leave en route), I showed up in class, 20 guys shouted in unison, "Hey, it's Goldberg!" What do you mean? Well, it seems that this group of New York wisenheimers had invented a twenty-first member of the group --Goldberg -- so that, each day, one guy could disappear, someone else would respond "Yo!" to Goldberg's name at roll call, and the head count would come out right. (Some of those wisenheimers are probably now writers for "Hogan's Heroes" -- they really knew how to fight a war.)

All I remember from the TA course is the instructor telling us that the time difference between Tokyo and Washington state was so many hours. Maybe ex-hossman Salami couldn't tell a canter from a gallop, and ex-radio operator Salami couldn't tell CUCUMBER from BETTY BOOP, but, dammit, he knew his time differences! He had the temerity to tell the instructor that the computation was an hour off -- we had to consider Pacific Daylight Saving Time. No, says the instructor, "the book says. . ." No matter that I had worked many a long, dull night in that intercept shack and I knew that when I got off duty, it was midnight in Tokyo. No, "the book" won.

TDY over, it was back to Fort Looie, as it was called. The only things I remember about the rest of my tour there include some useless

facts that I'll take with me to my grave, such as the routing number for "TOKYO AIR" -- 26907, according to a system in which the fourth digit was always a zero or a 5, and the fifth digit showed the total in noncarrying arithmetic. T also remember the things I did to fight off the boredom during off-duty hours between shifts while stuck in the boondocks. Like trying to tie my extra shoelaces in that funny braided way that only the Regular Army guys could master. Or taking a USAFI (U. S. Armed Forces Institute) correspondence course in Russian ("So that's how he started!"). Things like that. The last Christmas there, however, I made a lot of Christmas cards, including in each one a poem I wrote, imitating but not quite approximating Ogden Nash. One of the cards survived the holocaust of World War II and, strange to say, the poem in it was printed recently on the back cover of the Winter 1976 issue of the Phoenix Society's Phoenician. The reprint didn't bear a date or any word of explanation, so it looked to the uncritical eye like a "Christmas 1976" message. One NSAer even asked me a couple of times why I wrote the poem "as though" I was in the Signal Corps in 1945. I'd like to assure him, and anyone else who was confused by the Phoenician reprint, that it wasn't "as though" I was in Fort Looie in December of 1945 and until March 1946. I really was! Fred, believe me!

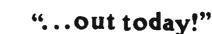


April 77 * CRYPTOLOG * Page 15

FOR OFFICIAL USE ONLY

DOCID: 4009793

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



(Continued from p. 3)

research not only delays publication of the message being researched, but all subsequent ones.

One factor that helps timeliness is any kind of background knowledge you happen to have -in history, literature, the comics. It is amazing how many odd kinds of information come in handy.

Within a reasonable

- period of time I have seen references to:
 the "Gray Eminence" (French history -
 - the reference puzzled one young translator very much),
 - "Adamastor" (Portuguese literature -- I tried hard to ungarble that),
 - "Fabius Cunctator" (Roman history),
 - Latin phrases -- obtorto collo, sic rebus stantibus, primus inter pares,
 - "the Prime Minister is required to steer between Scylla and Charybdis" (Greek mythology),
 - "These findings, unsatisfactory as they are to a Cartesian mind" (French science),
 - "He refuses to go to Canossa" (medieval history -- if the allusion is unknown, finding that Canossa is a small village in the Alps is not very helpful),
 - "the Draconian program passed by the Italian Parliament" (Greek history),
 - "the sword of Damocles hangs over his head" (Greek mythology),
 - "he is a quisling" (modern history),
 - "Yalta" (this is *not* Malta, as some younger translators are inclined to ungarble it, while admitting that it makes no sense).

Any or all of these, if not recognized by the translator, may take much of his time to research or, unfortunately, attempt to degarble. Such background information may come, not only from newspapers or collateral, but from paperback novels, science fiction, and, for all I know, from *True Story Magazine*. All of this is grist to a translator's mill.

Style

The word "style" suggests different things to different people. Some authors, translators, and editors -- especially those in the outside world -- think that style is concerned with making the text sound "elegant," with such things as never splitting an infinitive or changing the word "horse" to "equine quadruped." In the field of COMINT translation, however, "style" means just one thing -translating the foreign text into completely unambiguous English. It is *not* concerned with "elegant variations," and therefore, if a foreign writer, for example, uses the word "section" repeatedly, the translator sticks to it. Because the customer is not always able to ask the translator, "Does the word

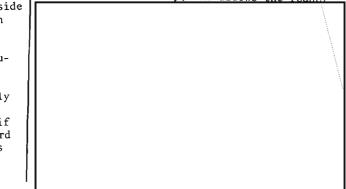
"A good translation," my Latin teacher used to say, "is one in which I can see where you got every word, but which reads as though it had been written in English." This is, of course, a goal to strive for, not to be attained. But, even so, in the interest of the readability I mentioned earlier. a translator should make sure that his adverbs clearly modify the right word, his adjective clauses attach to their antecedent nouns ("which" clauses dangling several words after their antecedents are, if not actually ambiguous, at least temporarily confusing). Try to avoid juxtaposing two words which normally go together if, in the passage in question, they do not belong together. True, if given enough time, the reader will work out the ambiguities, but in the intelligence field, time is of the essence. Many years ago I read

"Lake Leman lies by Chillon's walls. A thousand feet in depth below, Its massy waters meet and flow; Thus much the fathom line was sent From Chillon's snow-white battlement Which round about the wave enthralls; A double dungeon wall and wave Have made -- and like a living grave. . ."

It took me 20 years to get that passage parsed and realize that "wave" is not the object of the prepositional phrase "round about," but the subject of the verb "enthralls"; and that "double dungeon" is not a modifier of "wall," but the object of the verb ("wall and wave have made a double dungeon"). NSA's customers should not have to wait 20 years to realize what the translator is saying, nor even have to read a sentence twice. P.L. 86-36

EO 1.4.(c)

In the above excerpt, the words "dungeon" and "wall" form an unfortunate juxtaposition: they constitute a good concept and want to be read together. Poetic license allows the poet to write this way, and allows the reader



April 77 * CRYPTOLOG * Page 16

TOP SECRET UMBRA

Every language has its own characteristic translation problems. In Italian the abstract noun and the third-person impersonal subject are very popular. In English the active verb carries much more weight. Train yourself so that when you see, in the foreign text, "There is a tendency on the part of the Germans toward doubt," to make your pencil write "The Germans tend to doubt," without your having to think too much about why or how you are doing it. And don't allow yourself to fall into the habit of writing out a translation on a tablet sheet and then "Englishing" it. It wastes time. If translation into a dictaphone becomes more widespread, the ability to produce a fairly smooth translation first off will be essential. Listen mentally to your proposed translation to catch the awkward spots. "The statement states that the member states will make a statement on the state of their defense."

How to Use a Dictionary

For some time in this discussion I have been wanting to say something about dictionary usage. But I am not sure where is the best place to discuss it, because the dictionary is closely connected with all three essential elements of translation -- as a tool for accuracy and as a guide for style, but also, improperly used, as an enemy of timeliness. Yes, there is a wrong way to use a dictionary, namely, to believe that no word may be used in a translation unless it can be found in a dictionary as equivalent to the foreign word being translated. This erroneous belief leads to "dictionary hopping," the waste of time, and the use of a second- or third-choice word. I am sure that every checker, suggesting a different English word to a novice (or sometimes a not-so-novice) has heard, ad nauseam, "I wanted to say that, but I couldn't find it in the dictionary," or the opposite, "I know that the English doesn't make sense, but that's what it says in the dictionary!" And yet, even the dictionary compiler is human. I have seen some quaint, if not downright hilarious, English renderings of foreign words in dictionaries, even in the "standard" languages such as Italian, French, Spanish, or German.

To show the impossibility of relying wholly on dictionary synonyms without using critical judgment, I quote from "Teaching English as a Second Language," Toronto Education Quarterly, Winter/Spring 1968, as published in Today's Education -- NEA Journal:

"What happens when we consider only the words of a language and not their cultural connotations? One difficulty arose with electronic computers designed to translate from one language to another. The sentence 'The spirit is willing but the flesh is weak' was fed into a computer, translated into Russian, and then back into English. It came back as, 'The liquor is good but the meat is rotten.' The same process was followed with the headline, 'Mary suspended for youthful prank' and it came out as 'Mary hung for juvenile delinquency'. . . 'Out of sight, out of mind' went into Japanese and returned to English as 'invisible, insame.'

I am certain that, if one could have asked the computer, it would have said plaintively in each instance, "But that's what it said in the dictionary!"

The right way to use a dictionary is to consider its range of meaning or meanings (sometimes one word has two apparently unrelated meanings). Try to get a general idea of the root meaning. Look for examples of word usage. A dictionary says that a foreign word means "range." That's all! But is it "range" meaning the span of effectiveness, or "range" meaning a thing you cook on? Or maybe even the place where you fire at targets? What about "pot"? Is it what some people smoke, or what other people boil water in? Or is the place where things go when they fall apart?

No bilingual dictionary (say, an Italian-English dictionary) can list every English word that might be used to translate a foreign word in every conceivable context. Therefore, get used to the idea of referring to a dictionary in the foreign language, in which you read the definition of the foreign word, as speakers of that language define it, rather than the word's equivalents in English. After getting the *idea* from all the dictionaries available to you, select the English word for that idea out of your own vocabulary to match the context you have. And, if you know the word you want, but no bilingual dictionary gives anything near enough to satisfy you, look in a dictionary going in the opposite direction -- say, English-Italian. Often you will find the very word that you want.

And remember that usage changes. I noticed this particularly because I was away from Italian for several years, and when I first began working on it again, I spent half my time, it seemed, turning to somebody to ask, "Have you seen this word meaning this?" The answer usually was, "Yes. It has been meaning that for the last couple of years." For example, for 30 years *in vista di* regularly meant "in view of." Now, at least half the time, it seems to mean a completely different concept, "with a view to."

Furthermore, be sure you are looking for the right word in the dictionary. Can this verb form be derived from this infinitive? Can this

April 77 * CRYPTOLOG * Page 17

TOP SECRET UMBRA

DOCID: 4009.7936-36

EO 1.4.(c)

TOP SECRET UMBRA

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

noun be the plural of this one? Is there another dictionary entry from which the form in question could come? In Italian, testa (pl. teste) means "head," and testo (pl. testi) means "text." And then, to confuse one thoroughly, there is an adverb teste, meaning "just now." True, it has an accent mark in ordinary text. but since accent marks never appear is of no help. The ordinary reader may think that it should be completely obvious to the translator which of these three words was used, but in telegraphic, often garbled, text, things aren't always that easy.

To determine the root word, also consider the adjectives or articles that modify the noun. For example, La capitale italiana (feminine) refers to Rome, "the capital city," but il capitale italiano (masculine) is money, "Italian capital." Colpo means "blow," as in colpo di stato, "coup d'etat"; and colpa means "fault" or "blame."

At this point I would like to make a gripe. Current foreign-language education (or English education, for that matter) doesn't seem to teach grammar. One translator, to whom I pointed out that the verb was subjunctive, not indicative, and it made a difference (*perch*? followed by indicative means "because"; followed by subjunctive means "in order that"), looked at me wide-eyed and said, "But I haven't studied any French grammar since high school!" And he had been a French major in college. I'd like to know why or how.

Linguist's "Other Duties"?

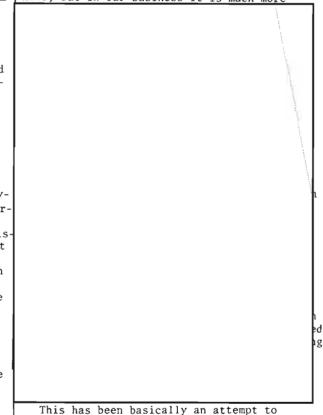
A major enemy of timeliness is piling everything on the translator. "The buck stops here" currently belongs on the translator's desk, not the President's. I know that it is nice for the adminis trator to have management information; in fact, it is rather necessary. But in most cases it doesn't require a linguist to supply it. Much has been written, and more said -- frequently blasphemously (by the translator) -- about the EXPERT sheet. The whole subject is currently in flux; while some of the burdens, such as writing "ØØ1" on virtually every translation, have been removed. Others have been added, and a report says that many others are in the offing. At present one major complaint is the effort -- and, usually, rewriting -- required to make the last carbon copy readable. One translator said recently, "I used to like to inish a translation so I could get a new one to start. Now I dread it, and put it off, because I'll have to make the EXPERT sheet."

Apart from the EXPERT sheet, there is the lack of translation sheets with the classification preprinted, and the lack of prenumbered paper for worksheet assignment. No reason

that I have heard given for these lacks seems to have any validity. The paper with preprinted classification, I was told, can be used incorrectly. But whether the paper is preprinted by the Agency print shop or the classification is prestamped in the section, the paper frequently has the classification already on it. And even if it doesn't, the translator who, by hand, writes TOP SECRET UMBRA 100 times correctly will frequently write it the hundred and first time, even it is not the correct classification.

"Does It Make Sense?"

Last but not least. "It's got to get out today," but it also has to make sense. If it does not, either it is wrong or you, the translator, are ignorant of some fact involved. and you'd better find out which. I have already said that you can't know everything, but you do know something and you should have and use common sense. A message should conform to what you already know and to its own internal logic. If man bites dog, it may be news, but in our business it is much more



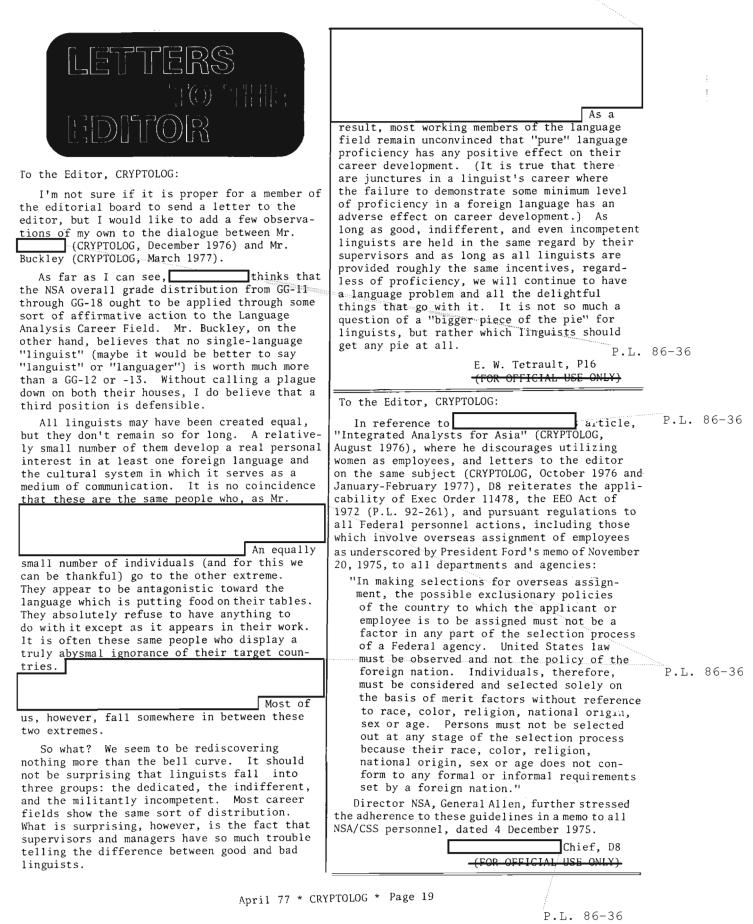
counteract what I feel is an *excessive* emphasis on research, research, and more research. It is not an excuse for sloppy or inaccurate translation. It all comes down to "It's got to get out today" -- or at least it ought to, in the best possible shape.

April 77 * CRYPTOLOG * Page 18

TOP SECRET UMBRA

FOR OFFICIAL USE ONLY

P.L. 86-36



FOR OFFICIAL USE ONLY

EO 1.4.(c) DOCID: 4009793 P.L. 86-36 -SECRET P.L. 86-36 To the Editor, CRYPTOLOG: To the Editor, CRYPTOLOG: Mr. Mason's article lists I noted in your January-February 1977 issue As President a letter from Ford emphasized in regard to selections for overseas assignments (see January 1977 WIN Newsletter), "United States law must be observed and not the policy of the foreign nation." If a woman applicant is the best qualified for a particular position, it is *illegal* to not accept concern is appreciated, I'm her. sure, but it is not necessary; there can be only a single standard for rating the performance. Elimination of double standards is what Women's Rights is all about. G515 Editor, WIN Newsletter P.S. Anyone wishing to subscribe to the WIN Newsletter can call me for information on extension 4235s. Anyone who would like to become a WIN member (membership includes a subscription to the Newsletter) can do so by sending \$3.00 to Rosalie L'Ecuyer, V362, 2E068, 5773s. (UNCLASSIFIED) To the Editor, CRYPTOLOG: We all owe Fred Mason a vote of thanks for his "Where Were We?" contribution to cryptologic history in the January-February 1977 issue. The centerfold idea makes it a useful desk reference aid (even though it can't compete with Burt Reynolds or Marilyn Monroe). Walter E. Landi (CONFIDENTIAL) To the Editor, CRYPTOLOG: Missing from Mr. Mason's /list of U.S. Navy stations is Poyner's Hill, N. C. During World War II it was located about 20 miles north of Nag's Head, on the Atlantic coast, east of Currituck Sound. I believe its designator was P. EO 1.4.(c)While the Intercept Station list includes some units without alpha-numeric designators, Also missing is the Navy station that was loP.L. 86-36 Part II does not. cated on the southern tip of Greenland during WWII. It lay to the northwest of Julianhaab, near the entrance/to a large fjord. I do not recall its name or designator (its callsign was maybe other readers can contribute dates/units to this worthwhile project? NTG). Should they send them to you? to P1? to E51? I suggest that the Navy station at Bainbridge Island, Wash., was turned over to the Coast 1 1 Guard well after 1945. I served as an inter-Editor's reply: cept operator there until mid-June 1946. Thank you for your word of caution and for your additions to Mr. Mason's compilation, which I have sent to him. Readers who have any more additions, corrections, etc. can send them either to: CRYPTOLOG, P1; or direct to the James R. McGrillies, F9203 author: Frederic O. Mason, Jr., P14. (CONFIDENTIAL) (SECRET - CCO) P.L. 86-36 P.L. 86-36 EO 1.4.(c) April 77 * CRYPTOLOG * Page 20 EO 1.4.(d)

Pl-Mar 77-S32-25187

TOP SECRET

-- ·

DOCID: 4009793

TOP SECRET

THIS DOCUMENT CONTAINS CODEWORD MATERIAL

