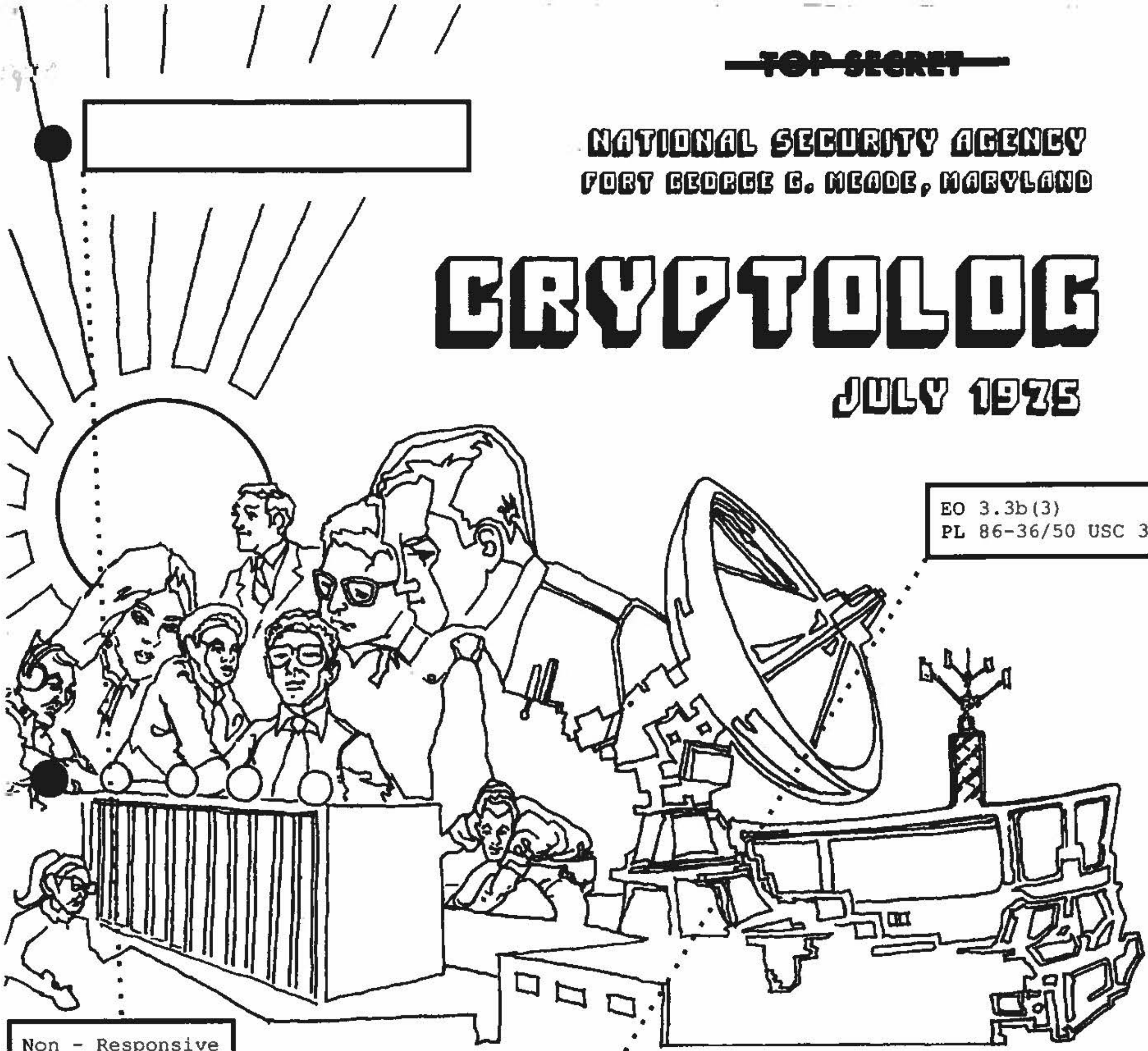
~~TOP SECRET~~

[redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JULY 1975



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

Non - Responsive

[redacted]

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM [illegible])~~
~~Exempt from [illegible] Category 2~~
~~Declassify Upon Notification by the Originator~~

THE WARSAW PACT

[redacted]

FREDERICK W. WALTON JR., A913

In recent years the Warsaw Pact has recognized the need for [redacted]

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

[redacted]

~~S~~TOO MAN~~X~~Y ~~F~~GARBLE~~R~~S

A Moral Tale for Cryptanalysts

By Harry G. Rosenblu~~m~~h

Some years ago a cryptanalyst working in the Latin American Section rejoiced. A link that had formerly carried only plaintext had suddenly popped up with a short cipher message.

"They probably wouldn't use anything tricky," said he, "so I should be able to break the system on this one message." He nearly did.

For the sake of the story, let's pretend that this is the text of the one message our cryptanalyst had to work with:

```
UDQVI PVHLV FSLGC TDQSD QXGMK

JABDQ VTPLQ GKDQH AMAEP LQGVH

APIYK DQLCQ CICSS EZOKH RCHMC

ZHRVE QPAYM OZZXA HGCIO HHSQV

HNZSA PDQCC NVQMP CDVGK LCMAE

PVCRV
```

The four-letter hits (MAEP and PLQG) and the repeated trigraphs (DQV and KDQ) with the distance between them divisible by 3 gave the first clue. In a relatively short time, the analyst handed me a worksheet with the decrypted text and cipher alphabets.

```
UDQVI PVHLV FSLGC TDQSD QXGMK
NOSOT ROSNO QUERE MOSLO SQROD

JABDQ VTPLQ GKDQH AMAEP LQGVH
UCUOS OEREB IDOSA LOTPR EBIOS

APIYK DQLCQ CICSS EZOKH RCHMC
CITAD OSENS VTELD GSZMA CEAXE

ZHRVE QPAYM OZZXA HGCIO HHSQV
SSTOP SILAF ZBSIC AREBZ JADSO

HNZSA PDQCC NVQMP CDVGK LCMAE
SPSDC IOSVN POBOI NFORM ENOTP

PVCRV
RONTO
```

Cipher:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Plain 1:	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*
Plain 2:	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*
Plain 3:	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*

Cipher:	S	T	U	V	W	X	Y	Z
Plain 1:	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*
Plain 2:	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*
Plain 3:	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*

I degarbled and translated the message as follows:

```
                         p     t
NOSOTROS NO QUEREMOS LOS Q̸RODUCU̸OS
 f            s    c                u
OE̸REBIDOS A LOT̸ PREB̸IOS CITADOS EN SV̸
   e ra   d   y r             a r
TELD̸GS̸Z̸MA C̸E AX̸ES̸ STOP SI LA FZ̸BS̸ICA
   a   e     re     u    c           s
REBZ̸JA D̸SOS PS̸D̸CIOS V̸N POB̸O INFORMENOT̸

PRONTO
```

(We don't want the products offered at the prices quoted in your telegram of yesterday. If the factory lowers the prices a bit, inform us at once.)

"Isn't that an awful lot of garbles for such a short message?" I was recalling the passage in MC-I about a 5-10% garble rate being acceptable, and 21 out of 130 is more than 16%. My friend muttered something about "a possibly inexperienced code clerk. . . poor transmission . . . you can't always depend upon percentages . . . 16% isn't that much more than 10% . . ." But I wasn't satisfied. Suppose, instead, that the message is all right, but the recovery isn't quite correct.

Not knowing what to suppose, I started from the degarbled text and the cipher message and reconstructed the three alphabets that the encrypter must have had in front of him. I ended up with this chart:

Plain:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Cipher 1:	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*X*	*Y*	*Z*
Cipher 2:	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*
Cipher 3:	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*

Plain:	S	T	U	V	X	Y	Z
Cipher 1:	*A*	*B*	*C*	*D*	*E*	*F*	*G*
Cipher 2:	*H*	*I*	*J*	*K*	*L*	*M*	*N*
Cipher 3:	*Q*	*R*	*S*	*T*	*U*	*V*	*X*

Those tricky characters had simply slid an alphabet without a W against itself, using the word *HOY* [today] under plain A as setting. Other three-letter words were used for setting subsequent messages; they could easily be spotted by writing the alphabets in encrypt order.

Moral: *Try to reproduce the cryptomaterials the cipher clerk used to encrypt the message.*

"RE-PSYCHLING" THE CODE CLERK

By Shirley Barton, F83

Mrs. Barton, who is currently working [redacted] submitted the following response to the editor's invitation to "match" Mr. Callimahos' WWII observations in the April 1975 issue.

Throughout the 1960's, the Vietnamese Communists were straightforward in their cryptographic habits and could be relied upon to be fairly secure [redacted] However, the VC code clerks, not unlike their Japanese counterparts in WWII (as discussed by Mr. Callimahos), had a peculiarity that gave the cryptanalyst that helpful boost.

In 1968 the VC began a gradual change from [redacted]

[redacted]

While there were indeed other features exploited by those engaged in the long-term, in-depth analysis of these communications, this particular one proved especially interesting to those of us engaged in the initial analysis of [redacted]

[redacted]